

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

J-C971 U.S. PTO
09/811459



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 5月30日

出 願 番 号

Application Number:

特願2000-160001

出 願 人

Applicant(s):

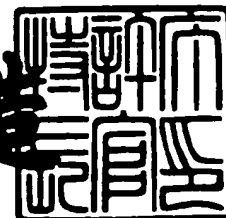
株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 3月 2日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2001-3015403

【書類名】 特許願

【整理番号】 H0000508

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区戸塚町 5 0 3 0 番地 株式会社日立製作所 ソフトウェア事業部内

【氏名】 桶屋 勝幸

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100096954

【弁理士】

【氏名又は名称】 矢島 保夫

【手数料の表示】

【予納台帳番号】 022781

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 楕円曲線暗号におけるスカラー倍計算方法及び装置、並びに記憶媒体

【特許請求の範囲】

【請求項 1】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー値のビットの値を判定するステップと、前記判定を行なったビットの値に依存せずに一定の回数及び一定の順序で楕円曲線上の演算を実行するステップとを含むことを特徴とするスカラー倍計算方法。

【請求項 2】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の 2 倍算を、楕円曲線上の加算を実行した後、楕円曲線上の 2 倍算を実行するという順序で行なうステップとを含むことを特徴とするスカラー倍計算方法。

【請求項 3】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の 2 倍算を、楕円曲線上の 2 倍算を実行した後、楕円曲線上の加算を実行するという順序で行なうステップとを含むことを特徴とするスカラー倍計算方法。

【請求項 4】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の 2 倍算を同時に実行するステップとを含むことを特徴とするスカラー

倍計算方法。

【請求項 5】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

楕円曲線上の加算を実行するステップと、前記スカラー値のビットの値を判定するステップと、楕円曲線上の 2 倍算を実行するステップとを含むことを特徴とするスカラー倍計算方法。

【請求項 6】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

楕円曲線上の加算及び楕円曲線上の 2 倍算の計算順序をランダム化するステップと、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の 2 倍算を、前記加算及び 2 倍算の計算順序をランダム化するステップによりランダム化された順序で行なうステップとを含むことを特徴とするスカラー倍計算方法。

【請求項 7】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の 2 倍算の計算順序をランダム化するステップと、楕円曲線上の加算及び楕円曲線上の 2 倍算を、前記加算及び 2 倍算の計算順序をランダム化するステップによりランダム化された順序で行なうステップとを含むことを特徴とするスカラー倍計算方法。

【請求項 8】

第 1 のデータから第 2 のデータを生成するデータ生成方法であって、請求項 1 から 7 の何れか 1 つに記載のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とするデータ生成方法。

【請求項 9】

データから署名データを生成する署名生成方法であって、請求項 1 から 7 の何

れか 1 つに記載のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする署名生成方法。

【請求項 1 0】

暗号化されたデータから復号化されたデータを生成する復号化方法であって、請求項 1 から 7 の何れか 1 つに記載のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする復号化方法。

【請求項 1 1】

楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算装置であって、

前記スカラー値のビットの値を判定するビット値判定手段と、楕円曲線上の加算を実行する加算演算手段と、楕円曲線上の 2 倍算を実行する 2 倍算演算手段とを具備し、

前記ビット値判定手段により前記スカラー値のビットの値を判定した後、前記加算演算手段及び 2 倍算演算手段により楕円曲線上の加算及び楕円曲線上の 2 倍算を一定の回数及び一定の順序で実行し、スカラー倍点を計算することを特徴とするスカラー倍計算装置。

【請求項 1 2】

請求項 1 から 7 の何れか 1 つに記載のスカラー倍計算方法に係るプログラムを格納したことを特徴とする記憶媒体。

【請求項 1 3】

請求項 1 から 7 の何れか 1 つに記載のスカラー倍計算方法において、前記楕円曲線としてモンゴメリ型楕円曲線を用いることを特徴とするスカラー倍計算方法。

【請求項 1 4】

請求項 1 から 7 の何れか 1 つに記載のスカラー倍計算方法において、前記楕円曲線として標数 2 の有限体上で定義された楕円曲線を用いることを特徴とするスカラー倍計算方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、コンピュータネットワークにおけるセキュリティ技術に関し、特に楕円曲線暗号における暗号処理方法及び装置並びに記憶媒体に関する。

【0002】

【従来の技術】

楕円曲線暗号は、N.Koblitz, V.S.Millerにより提案された公開鍵暗号の一種である。公開鍵暗号には、公開鍵と呼ばれる一般に公開してよい情報と、秘密鍵と呼ばれる秘匿しなければならない秘密情報がある。与えられたメッセージの暗号化や署名の検証には公開鍵を用い、与えられたメッセージの復号化や署名の作成には秘密鍵を用いる。楕円曲線暗号における秘密鍵は、スカラー値が担っている。また、楕円曲線暗号の安全性は、楕円曲線上の離散対数問題の求解が困難であることに由来している。ここで楕円曲線上の離散対数問題とは、楕円曲線上のある点 P とそのスカラー倍の点 dP が与えられたとき、スカラー値 d を求める問題である。ここにおいて、楕円曲線上の点とは、楕円曲線の定義方程式をみたす数の組をいう。楕円曲線上の点全体には、無限遠点という仮想的な点を単位元とした演算、すなわち楕円曲線上の加法が定義されている。そして、同じ点同士の楕円曲線上の加法のことを、特に楕円曲線上の2倍算という。ある点に対し、特定の回数だけ加法を行なうことをスカラー倍といい、その結果をスカラー倍点、その回数のことをスカラー値という。

【0003】

楕円曲線上の離散対数問題の求解の困難性が理論的に確立されてきている一方で、実際の実装においては秘密鍵等の秘密情報に関連する情報が暗号処理において漏洩する場合があります、その漏洩情報をもとに秘密情報を復元するといった、所謂パワーアナリシスという攻撃法が提案されている。

【0004】

DES(Data Encryption Standard)等の秘密情報を用いた暗号処理において、電圧変化を測定することで暗号処理経過を入手し、それをもとにして秘密情報を推察するという攻撃法が、P.Kocher, J.Jaffe, B.Jun Differential Power Analysis, Advances in Cryptology: Proceedings of CRYPTO '99, LNCS 1666, Spring

er-Verlag, (1999) pp.388-397. に記載されている。この攻撃法は、DPA(Differential Power Analysis)と呼ばれている。

【 0 0 0 5 】

楕円曲線暗号に対して上述の攻撃法を適用したものが、J.Coron, Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems, Cryptographic Hardware and Embedded Systems: Proceedings of CHES' 99, LNCS 1717, Springer-Verlag, (1999) pp.292-302. に記載されている。楕円曲線暗号において、与えられたメッセージの暗号化や復号化、乃至は署名の作成及びその検証は、楕円曲線演算を用いて行なう必要がある。特に、楕円曲線上のスカラー倍の計算は、秘密情報であるスカラー値を用いた暗号処理において用いられる。

【 0 0 0 6 】

また、モンゴメリ型楕円曲線 $BY^2 = X^3 + AX^2 + X$ ($A, B \in F_p$) を用いると標準型楕円曲線と呼ばれる通常用いる楕円曲線よりも高速に演算を実行できることが、P.L.Montgomery, Speeding the Pollard and Elliptic Curve Methods of Factorization, Math. Comp. 48 (1987) pp.243-264. に記載されている。これは、スカラー値の特定のビットの値に依存して、楕円曲線上の点の組 $(mP, (m+1)P)$ から点の組 $(2mP, (2m+1)P)$ 乃至は点の組 $((2m+1)P, (2m+2)P)$ を繰り返し計算するスカラー倍計算方法において、モンゴメリ型楕円曲線を利用することにより、加算及び2倍算の計算時間が短縮されることに由来する。

【 0 0 0 7 】

また、標数2の有限体上で定義された楕円曲線に対しても、モンゴメリ型楕円曲線におけるスカラー倍計算方法を適応させたスカラー倍計算方法並びにそれに用いる加算方法及び2倍算方法が、J.Lopez, R.Dahab, Fast Multiplication on Elliptic Curves over $GF(2^m)$ without Precomputation, Cryptographic Hardware and Embedded Systems: Proceedings of CHES' 99, LNCS 1717, Springer-Verlag, (1999) pp.316-327. に記載されている。このスカラー倍計算方法における加算及び2倍算の計算時間が短縮されることにより、標数2の有限体上で定義された楕円曲線における通常のスカラー倍計算方法と比べて、スカラー倍計算が

高速に実行できる。

【0008】

楕円曲線暗号に対するDPA攻撃の対処法の一つとして、ランダム化射影座標を用いる方法が、J.Coron, Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems, Cryptographic Hardware and Embedded Systems: Proceedings of CHES'99, LNCS 1717, Springer-Verlag, (1999) pp.292-302. に記載されている。これはスカラー倍計算において、特定の値が出現するかどうかを観測し、そこからスカラー値を割り出す攻撃法に対して、ランダムな値を乗ずることにより、特定の値が出現することを予測できなくする対処法である。

【0009】

【発明が解決しようとする課題】

上記従来技術の楕円曲線暗号は、DPA等のパワーアナリシスによる攻撃については考慮されていなかった。それゆえに、パワーアナリシスによる攻撃を和らげるためには、秘密情報を用いた暗号処理において、必要な計算以外に余分な計算を行なうなどして、暗号処理経過と秘密情報との依存関係を弱くしなければならなかった。そのため、暗号処理に必要な時間が増大し、ICカード等の計算速度の遅いコンピュータや、膨大な数の暗号処理をこなすサーバ等においては、暗号処理効率の低下が目立つ状態にあった。そのうえ、暗号処理経過と秘密情報との依存関係を完全に断ち切ることはできなかった。また、暗号処理効率を優先しようとするれば、パワーアナリシスによる攻撃を受け易く、秘密情報が漏洩する可能性があるという状態にあった。

【0010】

本発明の目的は、パワーアナリシス等により暗号処理経過が漏洩しても、秘密情報自体は漏洩せず、しかも高速に暗号処理を実行できる暗号処理方法及び装置並びに記憶媒体を提供すること、特に、秘密情報であるスカラー値から楕円曲線上のスカラー倍点を計算する計算経過からスカラー値の情報を引き出すことができないスカラー倍計算方法を提供することにある。

【0011】

【課題を解決するための手段】

上記目的を達成するため、本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー値のビットの値を判定するステップと、前記判定を行なったビットの値に依存せずに一定の回数及び一定の順序で楕円曲線上の演算を実行するステップとを含むことを特徴とする。

【 0 0 1 2 】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の 2 倍算を、楕円曲線上の加算を実行した後、楕円曲線上の 2 倍算を実行するという順序で行なうステップとを含むことを特徴とする。

【 0 0 1 3 】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の 2 倍算を、楕円曲線上の 2 倍算を実行した後、楕円曲線上の加算を実行するという順序で行なうステップとを含むことを特徴とする。

【 0 0 1 4 】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の 2 倍算を同時に実行するステップとを含むことを特徴とする。

【 0 0 1 5 】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、楕円曲線上の加算を実行するステップと、前記スカラー値のビットの値を判定するステップと、楕円曲線上の 2 倍算を実行するステップとを含むことを特徴とする。

【 0 0 1 6 】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカ

ラー倍点を計算するスカラー倍計算方法であって、楕円曲線上の加算及び楕円曲線上の2倍算の計算順序をランダム化するステップと、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の2倍算を、前記加算及び2倍算の計算順序をランダム化するステップによりランダム化された順序で行なうステップとを含むことを特徴とする。

【0017】

また本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー値のビットの値を判定するステップと、楕円曲線上の加算及び楕円曲線上の2倍算の計算順序をランダム化するステップと、楕円曲線上の加算及び楕円曲線上の2倍算を、前記加算及び2倍算の計算順序をランダム化するステップによりランダム化された順序で行なうステップとを含むことを特徴とする。

【0018】

また本発明は、第1のデータから第2のデータを生成するデータ生成方法であって、上述のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする。さらに、データから署名データを生成する署名生成方法であって、上述のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする。さらに、暗号化されたデータから復号化されたデータを生成する復号化方法であって、上述のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする。

【0019】

さらに、本発明は、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算装置であって、前記スカラー値のビットの値を判定するビット値判定手段と、楕円曲線上の加算を実行する加算演算手段と、楕円曲線上の2倍算を実行する2倍算演算手段とを具備し、前記ビット値判定手段により前記スカラー値のビットの値を判定した後、前記加算演算手段及び2倍算演算手段により楕円曲線上の加算及び楕円曲線上の2倍算を一定の回数及び一定の順序で実行し、スカラー倍点を計算することを特徴とする。

【0020】

さらに、本発明は、上述のスカラー倍計算方法に係るプログラムを格納したことを特徴とする記憶媒体にある。前記楕円曲線としてモンゴメリ型楕円曲線を用いるとよい。前記楕円曲線として標数 2 の有限体上で定義された楕円曲線を用いるとよい。

【0021】

【発明の実施の形態】

以下、本発明の実施の形態を図面を用いて説明する。

【0022】

図 1 1 は、本発明の実施の形態に係る暗号処理システムの構成図である。この暗号処理システム 1 1 0 1 は、例えば IC カード内に設けられ、暗号化（あるいは、復号化、署名の作成や検証）の際に、あるメッセージ（値）1 1 0 5 を入力すると所定の計算を行なってあるメッセージ（値）1 1 0 6 を出力する処理を行なう。暗号処理システム 1 1 0 1 は、暗号処理部 1 1 0 2、スカラー倍計算部 1 1 0 3、及び秘密情報格納部 1 1 0 4 を備えている。特に、本実施形態のスカラー倍計算部 1 1 0 3 は、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないものであり、これにより暗号処理システム 1 1 0 1 は、暗号処理経過が漏洩しても秘密情報は漏洩しないシステムになっている。

【0023】

図 1 6 は、図 1 1 の暗号処理システムにおける処理の流れを示すフローチャートである。図 1 7 は、図 1 1 の暗号処理システムにおける処理の流れを示すシーケンス図である。

【0024】

図 1 6 において、暗号処理システム 1 1 0 1 は、以下のようにして、与えられたメッセージ 1 1 0 5 から暗号処理を行なったメッセージ 1 1 0 6 を出力する。まず、メッセージ 1 1 0 5 を暗号処理システム 1 1 0 1 に入力すると、暗号処理部 1 1 0 2 がそれを受け取る（ステップ 1 6 0 1）。暗号処理部 1 1 0 2 は、スカラー倍計算部 1 1 0 3 に、入力メッセージ 1 1 0 5 に応じた楕円曲線上の点を与える（ステップ 1 6 0 2）。スカラー倍計算部 1 1 0 3 は、秘密情報格納部 1 1 0 4 より秘密情報であるスカラー値を受け取る（ステップ 1 6 0 3）。スカラー

一倍計算部 1103 は、受け取った点とスカラー値より、スカラー倍点を、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法で計算する（ステップ 1604）。スカラー倍計算部 1103 は、計算したスカラー倍点を暗号処理部 1102 に送る（ステップ 1605）。暗号処理部 1102 は、スカラー倍計算部 1103 より受け取ったスカラー倍点をもとにして暗号処理を行なう（ステップ 1606）。その結果を暗号処理を行なったメッセージ 1106 として出力する（ステップ 1607）。

【0025】

上記処理手順を図 17 のシーケンス図を用いて説明する。まず、暗号処理部 1701（図 11 の 1102）の実行する処理について説明する。暗号処理部 1701 は、入力メッセージを受け取る。暗号処理部 1701 は、入力メッセージをもとに楕円曲線上の点を選び、スカラー倍計算部 1702 に楕円曲線上の点を与え、そしてスカラー倍計算部 1702 からスカラー倍点を受け取る。暗号処理部 1701 は、受け取ったスカラー倍点を用いて暗号処理を行ない、その結果を出力メッセージとして出力する。

【0026】

次にスカラー倍計算部 1702（図 11 の 1103）の実行する処理について説明する。スカラー倍計算部 1702 は、暗号処理部 1701 より楕円曲線上の点を受け取る。スカラー倍計算部 1702 は、秘密情報格納部 1703 よりスカラー値を受け取る。スカラー倍計算部 1702 は、受け取った楕円曲線上の点及びスカラー値から、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法により、スカラー倍点を計算し、暗号処理部 1701 にスカラー倍点を送る。

【0027】

最後に秘密情報格納部 1703（図 11 の 1104）の実行する処理について説明する。秘密情報格納部 1703 は、スカラー倍計算部 1702 がスカラー倍を計算できるように、スカラー値をスカラー倍計算部 1702 に送る。

【0028】

スカラー倍計算部 1103 が実行するスカラー倍計算は、スカラー倍計算経過

が漏洩しても秘密情報であるスカラー値に関する情報は漏洩しないものである。そのため、暗号処理部 1 1 0 2 において、暗号処理を行なう際に暗号処理経過が漏洩したとしても、秘密情報であるスカラー値を扱っているのはスカラー倍計算部 1 1 0 3 のみであり、秘密情報に関する情報は漏洩しない。

【 0 0 2 9 】

次に、暗号処理システム 1 1 0 1 におけるスカラー倍計算部 1 1 0 3 の具体的な実施例を説明する。

【 0 0 3 0 】

図 2 は、暗号処理システム 1 1 0 1 における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第 1 実施例を示す図である。図 1 は、第 1 実施例のスカラー倍計算方法を示すフローチャートである。図 1 及び図 2 を参照して、第 1 実施例を説明する。

【 0 0 3 1 】

スカラー倍計算装置 2 0 1 では、点及びスカラー値 2 0 7 を入力し、以下の手順でスカラー倍 2 0 8 を出力する。ここで入力された点を P 、入力されたスカラー値を d 、出力するスカラー倍の点を dP で、それぞれ表すことにする。

【 0 0 3 2 】

ステップ 1 0 1 として、繰り返し判定部 2 0 6 において繰り返すか否かの判定を行なう為に、初期値として変数 I に 1 を代入する。ステップ 1 0 2 として、2 倍算演算部 2 0 4 により、点 P の 2 倍点 $2P$ を計算する。ステップ 1 0 3 として、スカラー倍計算装置 2 0 1 に入力された点 P とステップ 1 0 2 で求めた点 $2P$ を、点格納部 2 0 2 に点の組 $(P, 2P)$ として格納する。ステップ 1 0 4 として、繰り返し判定部 2 0 6 により、変数 I とスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ 1 1 3 へ行く。一致しなければステップ 1 0 5 へ行く。ステップ 1 0 5 として、変数 I を 1 増加させる。ステップ 1 0 6 として、ビット値判定部 2 0 5 により、スカラー値の I 番目のビットの値が 0 であるか 1 であるかを判定する。そのビットの値が 0 であればステップ 1 0 7 へ行く。そのビットの値が 1 であればステップ 1 1 0 へ行く。

【 0 0 3 3 】

ステップ107として、加算演算部203により、点格納部202に格納されている点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ108へ行く。ステップ108として、2倍算演算部204により、点格納部202に格納されている点の組 $(mP, (m+1)P)$ から点 mP の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ109へ行く。ステップ109として、ステップ108で求めた点 $2mP$ とステップ107で求めた点 $(2m+1)P$ を点格納部202に点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ104へ戻る。

【0034】

ステップ110として、加算演算部203により、点格納部202に格納されている点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ111へ行く。ステップ111として、2倍算演算部204により、点格納部202に格納されている点の組 $(mP, (m+1)P)$ から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ112へ行く。ステップ112として、ステップ110で求めた点 $(2m+1)P$ とステップ111で求めた点 $(2m+2)P$ を点格納部202に点の組 $((2m+1)P, (2m+2)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ104へ戻る。

【0035】

ステップ113として、点格納部202に格納されている点の組 $(mP, (m+1)P)$ から、点 mP をスカラー倍208として出力し、終了する。

【0036】

以上の手順により出力する値である点 mP が点 P のスカラー値 d によるスカラー倍の点 dP となることは、計算過程において格納されている点の組 $(mP, (m+1)P)$ の点 mP に対するスカラー値 m が、スカラー値 d における先頭 I ビットのビット列と一致することと、ステップ104においてステップ113へ行くと判定されるためには、 I とスカラー値 d のビット長が等しいことが必要であ

り、そのためスカラー値 m とスカラー値 d が一致することにより示される。

【 0 0 3 7 】

また、以上の手順によりスカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことの根拠は以下の通りである。計算経過からスカラー値に関する情報を得る為には、少なくとも、各々のスカラー値に対する計算経過の間に違いが存在しなければならない。まず、あるスカラー値と、そのスカラー値との間に特定のビットのみが異なるスカラー値とについて考える。特定ビットが異なるので、計算経過において特定の回数だけ繰り返した後のステップ 1 0 6 でのビット値の判定の後、ステップ 1 0 7 へ行くかステップ 1 1 0 へ行くかの違いが生じる。しかしながら、ステップ 1 0 7 へ行ってもステップ 1 1 0 へ行っても、共にその後で加算を行ない、次に 2 倍算を行ない、そしてその結果を点の組として格納するという手順をとり、ステップ 1 0 4 へと戻る為、計算経過としての差異は存在しない。したがって同一の計算経過をとるためスカラー値の情報は引き出すことはできない。

【 0 0 3 8 】

次に固定したビット長のスカラー値について考える。二つのビット長の同じスカラー値はいくつかのビットの値が異なる。値の異なるビットの数を k とし、与えられた 2 つのスカラー値をそれぞれ d_0 及び d_k とする。スカラー値 d_0 とスカラー値 d_k の間でビットの値が異なる最初のビットに対して、その値が d_k の対応するビットの値と等しく、その他のビットの値が d_0 の対応するビットの値と等しいようなスカラー値を d_1 とする。スカラー値 d_0 とスカラー値 d_1 は 1 ビットのみ値が異なる。次にスカラー値 d_1 とスカラー値 d_k の間でビットの値が異なる最初のビットに対して、その値が d_k の対応するビットの値と等しく、その他のビットの値が d_1 の対応するビットの値と等しいようなスカラー値を d_2 とする。スカラー値 d_1 とスカラー値 d_2 は 1 ビットのみ値が異なる。以下同様にしてスカラー値 d_{k-1} まで定める。スカラー値 d_0 とスカラー値 d_k は k ビットの値が異なるので、スカラー値 d_{k-1} とスカラー値 d_k は 1 ビットのみ値が異なる。したがって下付き指数の値が 1 だけ異なるスカラー値同士は 1 ビットのみ値が異なる。上述したように、1 ビットのみ値の異なるスカラー値同士に

においてはそれらの計算経過は同一となる。スカラー値 d_0 からスカラー値 d_k まで 1 ビットのみ値の異なるスカラー値の連鎖が存在するので、スカラー値 d_0 とスカラー値 d_k の計算経過は同一となる。ゆえに計算経過によりスカラー値の情報を引き出すことはできない。

【 0 0 3 9 】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、加算及び 2 倍算が高速に実行可能であり、通常用いる標準型楕円曲線よりも高速にスカラー倍計算が実行可能である。

【 0 0 4 0 】

標数 2 の有限体上で定義された楕円曲線に対しても、高速な加算及び 2 倍算の計算方法が知られており、上記手順において加算及び 2 倍算の計算にその計算方法を用いることにより、標数 2 の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能である。

【 0 0 4 1 】

図 5 は、図 1 1 の暗号処理システム 1 1 0 1 における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第 2 実施例を示す図である。図 4 は、第 2 実施例のスカラー倍計算方法を示すフローチャートである。図 4 及び図 5 を参照して、第 2 実施例を説明する。

【 0 0 4 2 】

スカラー倍計算装置 5 0 1 では、点及びスカラー値 5 0 7 を入力し、以下の手順でスカラー倍 5 0 8 を出力する。ステップ 4 0 1 として、繰り返し判定部 5 0 6 において繰り返すか否かの判定を行なう為に、初期値として変数 I に 1 を代入する。ステップ 4 0 2 として、2 倍算演算部 5 0 4 により、点 P の 2 倍点 $2P$ を計算する。ステップ 4 0 3 として、スカラー倍計算装置 5 0 1 に入力された点 P とステップ 4 0 2 で求めた点 $2P$ を、点格納部 5 0 2 に点の組 $(P, 2P)$ として格納する。ステップ 4 0 4 として、繰り返し判定部 5 0 6 により、変数 I とスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ 4 1 3 へ行く。一致しなければステップ 4 0 5 へ行く。ステップ 4 0 5 として、変数 I を 1 増加させる。ステップ 4 0 6 として、ビット値判定部 5 0 5 により、スカル

一値の I 番目のビットの値が 0 であるか 1 であるかを判定する。そのビットの値が 0 であればステップ 407 へ行く。そのビットの値が 1 であればステップ 410 へ行く。

【0043】

ステップ 407 として、2 倍算演算部 504 により、点格納部 502 に格納されている点の組 $(mP, (m+1)P)$ から点 mP の 2 倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ 408 へ行く。ステップ 408 として、加算演算部 503 により、点格納部 502 に格納されている点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ 409 へ行く。ステップ 409 として、ステップ 407 で求めた点 $2mP$ とステップ 408 で求めた点 $(2m+1)P$ を点格納部 502 に点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ 404 へ戻る。

【0044】

ステップ 410 として、2 倍算演算部 504 により、点格納部 502 に格納されている点の組 $(mP, (m+1)P)$ から点 $(m+1)P$ の 2 倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ 411 へ行く。ステップ 411 として、加算演算部 503 により、点格納部 502 に格納されている点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ 412 へ行く。ステップ 412 として、ステップ 411 で求めた点 $(2m+1)P$ とステップ 410 で求めた点 $(2m+2)P$ を点格納部 502 に点の組 $((2m+1)P, (2m+2)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ 404 へ戻る。

【0045】

ステップ 413 として、点格納部 502 に格納されている点の組 $(mP, (m+1)P)$ から、点 mP をスカラー倍 508 として出力し、終了する。

【0046】

以上の手順により出力する値である点 mP が点 P のスカラー値 d によるスカラ

一倍の点 dP となることは、第 1 実施例の場合と同様に示すことができる。

【 0 0 4 7 】

また、以上の手順によりスカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことの根拠は以下の通りである。ある特定のビットのみ値が異なる二つのスカラー値に対して、それらの計算経過が同一であることを示せば、他の部分は第一実施例における根拠と同様であるので、スカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことが示される。したがって、ある特定のビットのみ値が異なる二つのスカラー値について考える。ある特定のビットの値のみが異なるので、計算経過において特定の回数だけ繰り返した後のステップ 4 0 6 でのビット値の判定の後、ステップ 4 0 7 へ行くかステップ 4 1 0 へ行くかの違いが生じる。しかしながらステップ 4 0 7 へ行ってもステップ 4 1 0 へ行っても、共にその後で 2 倍算を行ない、次に加算を行ない、そしてその結果を点の組として格納するという手順をとり、ステップ 4 0 4 へと戻る為、計算経過としての差異は存在しない。ゆえにスカラー倍計算経過によりスカラー値の情報を引き出すことはできない。

【 0 0 4 8 】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、標準型楕円曲線よりも高速にスカラー倍計算が実行可能であることも、第 1 実施例と同様である。

【 0 0 4 9 】

標数 2 の有限体上で定義された楕円曲線に対しても、上記手順において加算及び 2 倍算の計算に高速な加算及び 2 倍算の計算方法を用いることにより、標数 2 の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能であることも、第 1 実施例と同様である。

【 0 0 5 0 】

図 7 は、図 1 1 の暗号処理システム 1 1 0 1 における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第 3 実施例を示す図である。図 6 は、第 3 実施例のスカラー倍計算方法を示すフローチャートである。図 6 及び図 7 を参照して、第 3 実施例を説明する。

【 0 0 5 1 】

スカラー倍計算装置 7 0 1 では、点及びスカラー値 7 0 7 を入力し、以下の手順でスカラー倍 7 0 8 を出力する。ステップ 6 0 1 として、繰り返し判定部 7 0 6 において繰り返すか否かの判定を行なう為に、初期値として変数 I に 1 を代入する。ステップ 6 0 2 として、2 倍算演算部 7 0 4 により、点 P の 2 倍点 $2P$ を計算する。ステップ 6 0 3 として、スカラー倍計算装置 7 0 1 に入力された点 P とステップ 6 0 2 で求めた点 $2P$ を、点格納部 7 0 2 に点の組 $(P, 2P)$ として格納する。ステップ 6 0 4 として、繰り返し判定部 7 0 6 により、変数 I とスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ 6 1 3 へ行く。一致しなければステップ 6 0 5 へ行く。ステップ 6 0 5 として、変数 I を 1 増加させる。ステップ 6 0 6 として、ビット値判定部 7 0 5 により、スカラー値の I 番目のビットの値が 0 であるか 1 であるかを判定する。そのビットの値が 0 であればステップ 6 0 7 へ行く。そのビットの値が 1 であればステップ 6 1 0 へ行く。

【 0 0 5 2 】

ステップ 6 0 7 として、加算及び 2 倍算演算部 7 0 3 により、点格納部 7 0 2 に格納されている点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ 及び点 mP の 2 倍算 $2(mP)$ を同時に行ない、点 $(2m+1)P$ 及び点 $2mP$ を計算する。その後ステップ 6 0 9 へ行く。ステップ 6 0 9 として、ステップ 6 0 7 で求めた点 $2mP$ と点 $(2m+1)P$ を点格納部 7 0 2 に点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ 6 0 4 へ戻る。

【 0 0 5 3 】

ステップ 6 1 0 として、加算及び 2 倍算演算部 7 0 3 により、点格納部 7 0 2 に格納されている点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ 及び点 $(m+1)P$ の 2 倍算 $2((m+1)P)$ を同時に行ない、点 $(2m+1)P$ 及び点 $(2m+2)P$ を計算する。その後ステップ 6 1 2 へ行く。ステップ 6 1 2 として、ステップ 6 1 0 で求めた点 $(2m+1)P$ と点 $(2m+2)P$ を点格納部 7 0 2 に点の組 $((2m+1)P, (2m+2)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステ

ップ 6 0 4 へ戻る。

【 0 0 5 4 】

ステップ 6 1 3 として、点格納部 7 0 2 に格納されている点の組 (mP , ($m+1$) P) から、点 mP をスカラー倍 7 0 8 として出力し、終了する。

【 0 0 5 5 】

以上の手順により出力する値である点 mP が点 P のスカラー値 d によるスカラー倍の点 dP となることは、第 1 実施例の場合と同様に示すことができる。

【 0 0 5 6 】

また、以上の手順によりスカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことの根拠は以下の通りである。ある特定のビットのみ値が異なる二つのスカラー値に対して、それらの計算経過が同一であることを示せば、他の部分は第一実施例における根拠と同様であるので、スカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことが示される。したがって、ある特定のビットのみ値が異なる二つのスカラー値について考える。ある特定のビットの値のみが異なるので、計算経過において特定の回数だけ繰り返した後のステップ 6 0 6 でのビット値の判定の後、ステップ 6 0 7 へ行くかステップ 6 1 0 へ行くかの違いが生じる。しかしながらステップ 6 0 7 へ行ってもステップ 6 1 0 へ行っても、共にその後で加算及び 2 倍算を同時に行ない、そしてそれらの結果を点の組として格納するという手順をとり、ステップ 6 0 4 へと戻る為、計算経過としての差異は存在しない。ゆえにスカラー倍計算経過によりスカラー値の情報を引き出すことはできない。

【 0 0 5 7 】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、標準型楕円曲線よりも高速にスカラー倍計算が実行可能であることも、第 1 実施例と同様である。

【 0 0 5 8 】

標数 2 の有限体上で定義された楕円曲線に対しても、上記手順において加算及び 2 倍算の計算に高速な加算及び 2 倍算の計算方法を用いることにより、標数 2 の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能であることも、第 1 実施例と同様である。

【 0 0 5 9 】

図 9 は、図 1 1 の暗号処理システム 1 1 0 1 における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第 4 実施例を示す図である。図 8 は、第 4 実施例のスカラー倍計算方法を示すフローチャートである。図 8 及び図 9 を参照して、第 4 実施例を説明する。

【 0 0 6 0 】

スカラー倍計算装置 9 0 1 では、点及びスカラー値 9 0 7 を入力し、以下の手順でスカラー倍 9 0 8 を出力する。ステップ 8 0 1 として、繰り返し判定部 9 0 6 において繰り返すか否かの判定を行なう為に、初期値として変数 I に 1 を代入する。ステップ 8 0 2 として、2 倍算演算部 9 0 4 により、点 P の 2 倍点 $2P$ を計算する。ステップ 8 0 3 として、スカラー倍計算装置 9 0 1 に入力された点 P とステップ 8 0 2 で求めた点 $2P$ を、点格納部 9 0 2 に点の組 $(P, 2P)$ として格納する。ステップ 8 0 4 として、繰り返し判定部 9 0 6 により、変数 I とスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ 8 1 3 へ行く。一致しなければステップ 8 0 5 へ行く。ステップ 8 0 5 として、変数 I を 1 だけ増加させる。ステップ 8 0 6 として、加算演算部 9 0 3 により、点格納部 9 0 2 に格納されている点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。ステップ 8 0 7 として、ビット値判定部 9 0 5 により、スカラー値の I 番目のビットの値が 0 であるか 1 であるかを判定する。そのビットの値が 0 であればステップ 8 0 8 へ行く。そのビットの値が 1 であればステップ 8 1 1 へ行く。

【 0 0 6 1 】

ステップ 8 0 8 として、2 倍算演算部 9 0 4 により、点格納部 9 0 2 に格納されている点の組 $(mP, (m+1)P)$ から点 mP の 2 倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ 8 0 9 へ行く。ステップ 8 0 9 として、ステップ 8 0 8 で求めた点 $2mP$ とステップ 8 0 6 で求めた点 $(2m+1)P$ を点格納部 9 0 2 に点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ 8 0 4 へ戻る。ステップ 8 1 1 として、2 倍算演算部 9 0 4 により、点格納部 9 0 2 に格納されている点の組

(mP , $(m+1)P$) から点 $(m+1)P$ の 2 倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ 812 へ行く。ステップ 812 として、ステップ 806 で求めた点 $(2m+1)P$ とステップ 811 で求めた点 $(2m+2)P$ を点格納部 902 に点の組 $((2m+1)P, (2m+2)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ 804 へ戻る。

【0062】

ステップ 813 として、点格納部 902 に格納されている点の組 $(mP, (m+1)P)$ から、点 mP をスカラー倍 908 として出力し、終了する。

【0063】

以上の手順により出力する値である点 mP が点 P のスカラー値 d によるスカラー倍の点 dP となることは、第 1 実施例の場合と同様に示すことができる。

【0064】

また、以上の手順によりスカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことの根拠は以下の通りである。ある特定のビットのみ値が異なる二つのスカラー値に対して、それらの計算経過が同一であることを示せば、他の部分は第一実施例における根拠と同様であるので、スカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことが示される。したがって、ある特定のビットのみ値が異なる二つのスカラー値について考える。ある特定のビットの値のみが異なるので、計算経過において特定の回数だけ繰り返した後のステップ 807 でのビット値の判定の後、ステップ 808 へ行くかステップ 811 へ行くかの違いが生じる。しかしながらステップ 808 へ行ってもステップ 811 へ行っても、共にその後で 2 倍算を行ない、そしてその結果を加算の結果とともに点の組として格納するという手順をとり、ステップ 804 へと戻る為、計算経過としての差異は存在しない。ゆえにスカラー倍計算経過によりスカラー値の情報を引き出すことはできない。

【0065】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、標準型楕円曲線よりも高速にスカラー倍計算が実行可能であることも、第 1 実施例と同様である。

【0066】

標数2の有限体上で定義された楕円曲線に対しても、上記手順において加算及び2倍算の計算に高速な加算及び2倍算の計算方法を用いることにより、標数2の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能であることも、第1実施例と同様である。

【0067】

図15は、図11の暗号処理システム1101における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第5実施例を示す図である。図12、図13及び図14は、第5実施例のスカラー倍計算方法を示すフローチャートである。図12～図15を参照して、第5実施例を説明する。

【0068】

スカラー倍計算装置1501では、点及びスカラー値1507を入力し、以下の手順でスカラー倍1508を出力する。ステップ1201として、繰り返し判定部1506において繰り返すか否かの判定を行なう為に、初期値として変数Iに1を代入する。ステップ1202として、2倍算演算部1504により、点Pの2倍点2Pを計算する。ステップ1203として、スカラー倍計算装置1501に入力された点Pとステップ1202で求めた点2Pを、点格納部1502に点の組(P, 2P)として格納する。ステップ1204として、繰り返し判定部1506により、変数Iとスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ1213へ行く。一致しなければステップ1205へ行く。ステップ1205として、変数Iを1増加させる。ステップ1206として、演算ランダム化部1509により、加算及び2倍算の計算順序をランダム化する。加算、2倍算の順序で計算を実行する場合はステップ1301へ行く。2倍算、加算の順序で計算を実行する場合はステップ1401へ行く。

【0069】

ステップ1301として、ビット値判定部1505により、スカラー値のI番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ1302へ行く。そのビットの値が1であればステップ1305へ行

の計算順序をランダム化する。加算、2倍算の順序で計算を実行する場合はステップ2405へ行く。2倍算、加算の順序で計算を実行する場合はステップ2402へ行く。

【0087】

ステップ2402として、2倍算演算部2504により、点格納部2502に格納されている点の組(mP , $(m+1)P$)から点 mP の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ2403へ行く。ステップ2403として、加算演算部2503により、点格納部2502に格納されている点の組(mP , $(m+1)P$)から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ2404へ行く。

【0088】

ステップ2405として、加算演算部2503により、点格納部2502に格納されている点の組(mP , $(m+1)P$)から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ2406へ行く。ステップ2406として、2倍算演算部2504により、点格納部2502に格納されている点の組(mP , $(m+1)P$)から点 mP の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ2404へ行く。

【0089】

ステップ2404として、ステップ2402乃至はステップ2406で求めた点 $2mP$ とステップ2403乃至はステップ2405で求めた点 $(2m+1)P$ を点格納部2502に点の組($2mP$, $(2m+1)P$)として、点の組(mP , $(m+1)P$)の代わりに格納する。その後ステップ2204へ戻る。

【0090】

ステップ2213として、点格納部2502に格納されている点の組(mP , $(m+1)P$)から、点 mP をスカラー倍2508として出力し、終了する。

【0091】

以上の手順により出力する値である点 mP が点 P のスカラー値 d によるスカラー倍の点 dP となることは、第1実施例の場合と同様に示すことができる。

【0092】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、加算及び2倍算が高速に実行可能であり、通常用いる標準型楕円曲線よりも高速にスカラー倍計算が実行可能である。

【0093】

標数2の有限体上で定義された楕円曲線に対しても、上記手順において加算及び2倍算の計算に高速な加算及び2倍算の計算方法を用いることにより、標数2の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能である。

【0094】

図27は、図11の暗号処理システム1101における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第7実施例を示す図である。図26は、第7実施例のスカラー倍計算方法を示すフローチャートである。図26及び図27を参照して、第7実施例を説明する。

【0095】

スカラー倍計算装置2701では、点及びスカラー値2707を入力し、以下の手順でスカラー倍2708を出力する。ステップ2601として、繰り返し判定部2706において繰り返すか否かの判定を行なう為に、初期値として変数Iに1を代入する。ステップ2614として、ランダム化射影座標変換部2709により、乱数kを生成する。ステップ2615として、ランダム化射影座標変換部2709により、ステップ2614で生成したkを用いて、点Pを射影座標において、 $P = (kx, ky, k)$ と表す。ここで点Pは、アフィン座標では、 $P = (x, y)$ と表されとする。ステップ2602として、2倍算演算部2704により、ステップ2615で (kx, ky, k) と表された点Pの2倍点2Pを計算する。ステップ2603として、スカラー倍計算装置2701に入力され、ステップ2615で (kx, ky, k) と表された点Pと、ステップ2602で求めた点2Pを、点格納部2702に点の組 $(P, 2P)$ として格納する。

【0096】

ステップ2604として、繰り返し判定部2706により、変数Iとスカラー

値のビット長とが一致するかどうかを判定し、一致すればステップ 2 6 1 3 へ行く。一致しなければステップ 2 6 0 5 へ行く。ステップ 2 6 0 5 として、変数 I を 1 増加させる。ステップ 2 6 0 6 として、ビット値判定部 2 7 0 5 により、スカラー値の I 番目のビットの値が 0 であるか 1 であるかを判定する。そのビットの値が 0 であればステップ 2 6 0 7 へ行く。そのビットの値が 1 であればステップ 2 6 1 0 へ行く。

【 0 0 9 7 】

ステップ 2 6 0 7 として、加算演算部 2 7 0 3 により、点格納部 2 7 0 2 に格納されている点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ 2 6 0 8 へ行く。ステップ 2 6 0 8 として、2 倍算演算部 2 7 0 4 により、点格納部 2 7 0 2 に格納されている点の組 $(mP, (m+1)P)$ から点 mP の 2 倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ 2 6 0 9 へ行く。ステップ 2 6 0 9 として、ステップ 2 6 0 8 で求めた点 $2mP$ とステップ 2 6 0 7 で求めた点 $(2m+1)P$ を点格納部 2 7 0 2 に点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ 2 6 0 4 へ戻る。

【 0 0 9 8 】

ステップ 2 6 1 0 として、加算演算部 2 7 0 3 により、点格納部 2 7 0 2 に格納されている点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ 2 6 1 1 へ行く。ステップ 2 6 1 1 として、2 倍算演算部 2 7 0 4 により、点格納部 2 7 0 2 に格納されている点の組 $(mP, (m+1)P)$ から点 $(m+1)P$ の 2 倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ 2 6 1 2 へ行く。ステップ 2 6 1 2 として、ステップ 2 6 1 0 で求めた点 $(2m+1)P$ とステップ 2 6 1 1 で求めた点 $(2m+2)P$ を点格納部 2 7 0 2 に点の組 $((2m+1)P, (2m+2)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ 2 6 0 4 へ戻る。

【 0 0 9 9 】

ステップ 2 6 1 3 として、点格納部 2 7 0 2 に格納されている点の組 (mP , $(m+1)P$) から、点 mP をスカラー倍 2 7 0 8 として出力し、終了する。

【0 1 0 0】

以上の手順により出力する値である点 mP が点 P のスカラー値 d によるスカラー倍の点 dP となることは、第 1 実施例の場合と同様に示すことができる。

【0 1 0 1】

また、以上の手順によりスカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報が漏洩しないことの根拠は、第 1 実施例における根拠と同様である。そのうえ、スカラー倍計算において、特定の値が出現するか否かを観測し、そこからスカラー値を割り出す攻撃法に対しても、最初にランダムな値を乗じている為、特定の値の出現を予測できなくなるので、そのような攻撃法に対しても、スカラー値に関する情報が漏洩しないことがわかる。

【0 1 0 2】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、標準型楕円曲線よりも高速にスカラー倍計算が実行可能であることも、第 1 実施例と同様である。

【0 1 0 3】

標数 2 の有限体上で定義された楕円曲線に対しても、上記手順において加算及び 2 倍算の計算に高速な加算及び 2 倍算の計算方法を用いることにより、標数 2 の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能であることも、第 1 実施例と同様である。

【0 1 0 4】

図 2 8 は、図 2 7 のランダム化射影座標変換部 2 7 0 9 として使用するランダム化射影座標変換装置の一実施例を示す図である。図 2 9 は、このランダム化射影座標変換装置におけるランダム化射影座標変換方法を示すフローチャートである。

【0 1 0 5】

ランダム化射影座標変換装置 2 8 0 1 では、楕円曲線上の点 2 8 0 5 を入力し、以下の手順でランダム化射影座標で表された点 2 8 0 6 を出力する。ステップ 2 9 0 1 として、座標判定部 2 8 0 2 により、与えられた楕円曲線上の点 2 8 0

5 がアフィン座標で表されているか、それとも射影座標で表されているかを判定する。アフィン座標で表されていればステップ 2 9 0 2 へ行く。射影座標で表されていればステップ 2 9 0 3 へ行く。ステップ 2 9 0 2 として、次のようにしてアフィン座標で表された点を射影座標で表す。アフィン座標で表された点を (x, y) とすると、射影座標として $(x, y, 1)$ と表す。

【0106】

ステップ 2 9 0 3 として、乱数生成部 2 8 0 3 により、乱数 k を生成する。ステップ 2 9 0 4 として、射影座標変換部 2 8 0 4 により、次のようにして射影座標で表された与えられた点をランダム化射影座標により表す。与えられた点を (x, y, z) とすると、乱数生成部 2 8 0 3 で生成された乱数 k を、各座標に乘じ、 (kx, ky, kz) と表し、ランダム化射影座標で表された点 2 8 0 6 として出力する。

【0107】

射影座標においては、0 以外の任意の数 k により各座標を乗じても、同じ点と見做す。すなわち、 (x, y, z) と (kx, ky, kz) は同じ点を表している。

【0108】

また、メモリ等の節約の為、ステップ 2 9 0 2 の $(x, y, 1)$ は実際に格納しなくとも、仮想的に $(x, y, 1)$ と表されていると考え、ステップ 2 9 0 4 で (kx, ky, k) と表す際に、実際に格納を行なってもよい。

【0109】

図 3 は、図 1 1 の本実施形態の暗号処理システムを署名作成装置として利用する場合の構成を示す。図 1 1 における暗号処理部 1 1 0 2 は、図 3 の署名作成装置 3 0 1 では署名部 3 0 2 になる。図 1 8 は、図 3 の署名作成装置における処理の流れを示すフローチャートである。図 1 9 は、図 3 の署名作成装置における処理の流れを示すシーケンス図である。

【0110】

図 1 8 において、署名作成装置 3 0 1 は、以下のようにして、与えられたメッセージ 3 0 5 から署名が付随しているメッセージ 3 0 6 を出力する。メッセージ

305を署名作成装置301に入力すると、署名部302がそれを受け取る（ステップ1801）。署名部302は、スカラー倍計算部303に、入力メッセージ305に応じた楕円曲線上の点を与える（ステップ1802）。スカラー倍計算部303は、秘密情報格納部304より秘密情報であるスカラー値を受け取る（ステップ1803）。スカラー倍計算部303は、受け取った点とスカラー値より、スカラー倍点を、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法で計算する（ステップ1804）。スカラー倍計算部303は、計算したスカラー倍点を署名部302に送る（ステップ1805）。署名部302は、スカラー倍計算部303より受け取ったスカラー倍点をもとにして署名作成処理を行なう（ステップ1806）。その結果を署名が付随したメッセージ306として出力する（ステップ1807）。

【0111】

上記処理手順を図19のシーケンス図を用いて説明する。まず、署名部1901（図3の302）の実行する処理について説明する。署名部1901は、入力メッセージを受け取る。署名部1901は、入力メッセージをもとに楕円曲線上の点を選び、スカラー倍計算部1902に楕円曲線上の点を与え、そしてスカラー倍計算部1902からスカラー倍点を受け取る。署名部1901は、受け取ったスカラー倍点を用いて署名作成処理を行ない、その結果を出力メッセージとして出力する。

【0112】

次にスカラー倍計算部1902（図3の303）の実行する処理について説明する。スカラー倍計算部1902は、署名部1901より楕円曲線上の点を受け取る。スカラー倍計算部1902は、秘密情報格納部1903よりスカラー値を受け取る。スカラー倍計算部1903は、受け取った楕円曲線上の点及びスカラー値から、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法により、スカラー倍点を計算し、署名部1901にスカラー倍点を送る。

【0113】

最後に秘密情報格納部1903（図3の304）の実行する処理について説明する。秘密情報格納部1903は、スカラー倍計算部1902がスカラー倍を計

算できるように、スカラー値をスカラー倍計算部 1 9 0 2 に送る。

【 0 1 1 4 】

スカラー倍計算部 3 0 3 が実行するスカラー倍計算は、上述した第 1 ～第 7 実施例で説明したものがそのまま適用される。したがって、このスカラー倍計算は、スカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報は漏洩しないものである。そのため署名部 3 0 2 において、署名作成処理を行なう際に署名作成処理経過が漏洩したとしても、秘密情報であるスカラー値を扱っているのはスカラー倍計算部 3 0 3 のみであり、秘密情報に関する情報は漏洩しない。

【 0 1 1 5 】

図 1 0 は、図 1 1 の本実施形態の暗号処理システムを復号化装置として利用する場合の構成を示す。図 1 1 における暗号処理部 1 1 0 2 は、図 1 0 の復号化装置 1 0 0 1 では復号部 1 0 0 2 になる。図 2 0 は、図 1 0 の復号化装置における処理の流れを示すフローチャートである。図 2 1 は、図 1 0 の復号化装置における処理の流れを示すシーケンス図である。

【 0 1 1 6 】

図 2 0 において、復号化装置 1 0 0 1 は、以下のようにして、与えられたメッセージ 1 0 0 5 から復号化されたメッセージ 1 0 0 6 を出力する。メッセージ 1 0 0 5 を復号化装置 1 0 0 1 に入力すると、復号部 1 0 0 2 がそれを受け取る（ステップ 2 0 0 1）。復号部 1 0 0 2 は、スカラー倍計算部 1 0 0 3 に、入力メッセージ 1 0 0 5 に応じた楕円曲線上の点を与える（ステップ 2 0 0 2）。スカラー倍計算部 1 0 0 3 は、秘密情報格納部 1 0 0 4 より秘密情報であるスカラー値を受け取る（ステップ 2 0 0 3）。スカラー倍計算部 1 0 0 3 は、受け取った点とスカラー値より、スカラー倍点を、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法で計算する（ステップ 2 0 0 4）。スカラー倍計算部 1 0 0 3 は、計算したスカラー倍点を復号部 1 0 0 2 に送る（ステップ 2 0 0 5）。復号部 1 0 0 2 は、スカラー倍計算部 1 0 0 3 より受け取ったスカラー倍点をもとにして復号化処理を行なう（ステップ 2 0 0 6）。その結果を復号化されたメッセージ 1 0 0 6 として出力する（ステップ 2 0 0 7）。

【0117】

上記処理手順を図21のシーケンス図を用いて説明する。まず、復号部2101（図10の1002）の実行する処理について説明する。復号部2101は、入力メッセージを受け取る。復号部2101は、入力メッセージをもとに楕円曲線上の点を選び、スカラー倍計算部2102に楕円曲線上の点を与え、そしてスカラー倍計算部2102からスカラー倍点を受け取る。復号部2101は、受け取ったスカラー倍点を用いて復号化処理を行ない、その結果を出力メッセージとして出力する。

【0118】

次にスカラー倍計算部2102（図10の1003）の実行する処理について説明する。スカラー倍計算部2102は、復号部2101より楕円曲線上の点を受け取る。スカラー倍計算部2102は、秘密情報格納部2103よりスカラー値を受け取る。スカラー倍計算部2103は、受け取った楕円曲線上の点及びスカラー値から、スカラー倍計算経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法により、スカラー倍点を計算し、復号部2101にスカラー倍点を送る。

【0119】

最後に秘密情報格納部2103（図10の1004）の実行する処理について説明する。秘密情報格納部2103は、スカラー倍計算部2102がスカラー倍を計算できるように、スカラー値をスカラー倍計算部2102に送る。

【0120】

スカラー倍計算部1003が実行するスカラー倍計算は、上述した第1～第7実施例で説明したものがそのまま適用される。したがって、このスカラー倍計算は、スカラー倍計算経過が漏洩しても秘密情報であるスカラー値に関する情報は漏洩しないものである。そのため復号部1002において、復号化処理を行なう際に復号化処理経過が漏洩したとしても、秘密情報であるスカラー値を扱っているのはスカラー倍計算部1003のみであり、秘密情報に関する情報は漏洩しない。

【0121】

【発明の効果】

以上述べたように、本発明によれば、暗号処理システムにおける秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても、暗号処理経過と秘密情報との依存関係が完全に断ち切られているので、秘密情報は漏洩しない。また、使用する楕円曲線をモンゴメリ型楕円曲線とすることで暗号処理の高速化を図ることができる。同様に、楕円曲線として標数 2 の有限体上で定義された楕円曲線を用いることで暗号処理の高速化を図ることができる。

【図面の簡単な説明】

【図 1】

本発明の第 1 実施例のスカラー倍計算方法を示すフローチャート図である。

【図 2】

第 1 実施例のスカラー倍計算方法及び装置における処理の流れを示す図である。

【図 3】

本発明の実施の形態に係る署名作成装置の構成図である。

【図 4】

本発明の第 2 実施例のスカラー倍計算方法を示すフローチャート図である。

【図 5】

第 2 実施例のスカラー倍計算方法及び装置における処理の流れを示す図である。

【図 6】

本発明の第 3 実施例のスカラー倍計算方法を示すフローチャート図である。

【図 7】

第 3 実施例のスカラー倍計算方法及び装置における処理の流れを示す図である。

【図 8】

本発明の第 4 実施例のスカラー倍計算方法を示すフローチャート図である。

【図 9】

第 4 実施例のスカラー倍計算方法及び装置における処理の流れを示す図である。

【図 1 0】

本発明の実施の形態に係る復号化装置の構成図である。

【図 1 1】

本発明の実施の形態に係る暗号処理システムの構成図である。

【図 1 2】

本発明の第 5 実施例のスカラー倍計算方法を示すフローチャート図である。

【図 1 3】

本発明の第 5 実施例のスカラー倍計算方法を示すフローチャート図である。

【図 1 4】

本発明の第 5 実施例のスカラー倍計算方法を示すフローチャート図である。

【図 1 5】

第 5 実施例のスカラー倍計算方法及び装置における処理の流れを示す図である。

【図 1 6】

図 1 1 の暗号処理システムにおける暗号処理方法を示すフローチャート図である。

【図 1 7】

図 1 1 の暗号処理システムにおける処理の流れを示すシーケンス図である。

【図 1 8】

図 3 の署名作成装置における署名作成方法を示すフローチャート図である。

【図 1 9】

図 3 の署名作成装置における処理の流れを示すシーケンス図である。

【図 2 0】

図 1 0 の復号化装置における復号化方法を示すフローチャート図である。

【図 2 1】

図 1 0 の復号化装置での処理の流れを示すシーケンス図である。

【図 2 2】

本発明の第 6 実施例のスカラー倍計算方法を示すフローチャート図である。

【図 2 3】

本発明の第 6 実施例のスカラー倍計算方法を示すフローチャート図である。

【図 2 4】

本発明の第 6 実施例のスカラー倍計算方法を示すフローチャート図である。

【図 2 5】

第 6 実施例のスカラー倍計算方法及び装置における処理の流れを示す図である。

【図 2 6】

本発明の第 7 実施例のスカラー倍計算方法を示すフローチャート図である。

【図 2 7】

第 7 実施例のスカラー倍計算方法及び装置における処理の流れを示す図である。

【図 2 8】

図 2 7 のランダム化射影座標変換装置を示す図である。

【図 2 9】

ランダム化射影座標変換装置におけるランダム化射影座標変換方法を示すフローチャート図である。

【符号の説明】

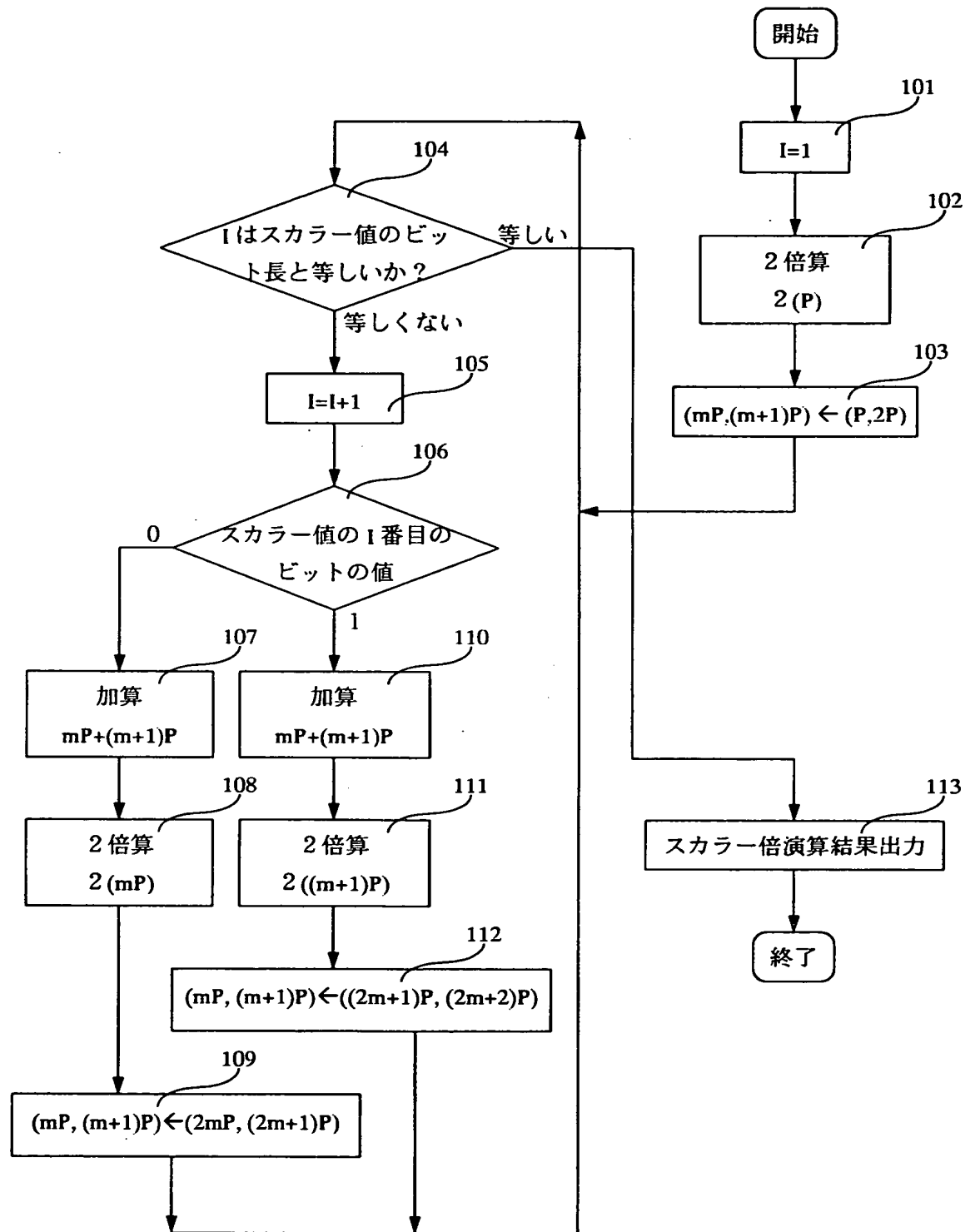
- 2 0 1 スカラー倍計算装置
- 2 0 2 点格納部
- 2 0 3 加算演算部
- 2 0 4 2 倍算演算部
- 2 0 5 ビット値判定部
- 2 0 6 繰り返し判定部
- 2 0 7 点及びスカラー値
- 2 0 8 スカラー倍
- 3 0 1 署名作成装置
- 3 0 2 署名部
- 3 0 3 スカラー倍計算部

- 3 0 4 秘密情報格納部
- 3 0 5 入力メッセージ
- 3 0 6 出力メッセージ
- 7 0 1 スカラー倍計算装置
- 7 0 2 点格納部
- 7 0 3 加算及び 2 倍算演算部
- 7 0 4 2 倍算演算部
- 7 0 5 ビット値判定部
- 7 0 6 繰り返し判定部
- 7 0 7 点及びスカラー値
- 7 0 8 スカラー倍
- 1 0 0 1 復号化装置
- 1 0 0 2 復号化部
- 1 0 0 3 スカラー倍計算部
- 1 0 0 4 秘密情報格納部
- 1 0 0 5 入力メッセージ
- 1 0 0 6 出力メッセージ
- 1 1 0 1 暗号処理システム
- 1 1 0 2 暗号処理部
- 1 1 0 3 スカラー倍計算部
- 1 1 0 4 秘密情報格納部
- 1 1 0 5 入力メッセージ
- 1 1 0 6 出力メッセージ
- 1 5 0 1 スカラー倍計算装置
- 1 5 0 2 点格納部
- 1 5 0 3 加算演算部
- 1 5 0 4 2 倍算演算部
- 1 5 0 5 ビット値判定部
- 1 5 0 6 繰り返し判定部

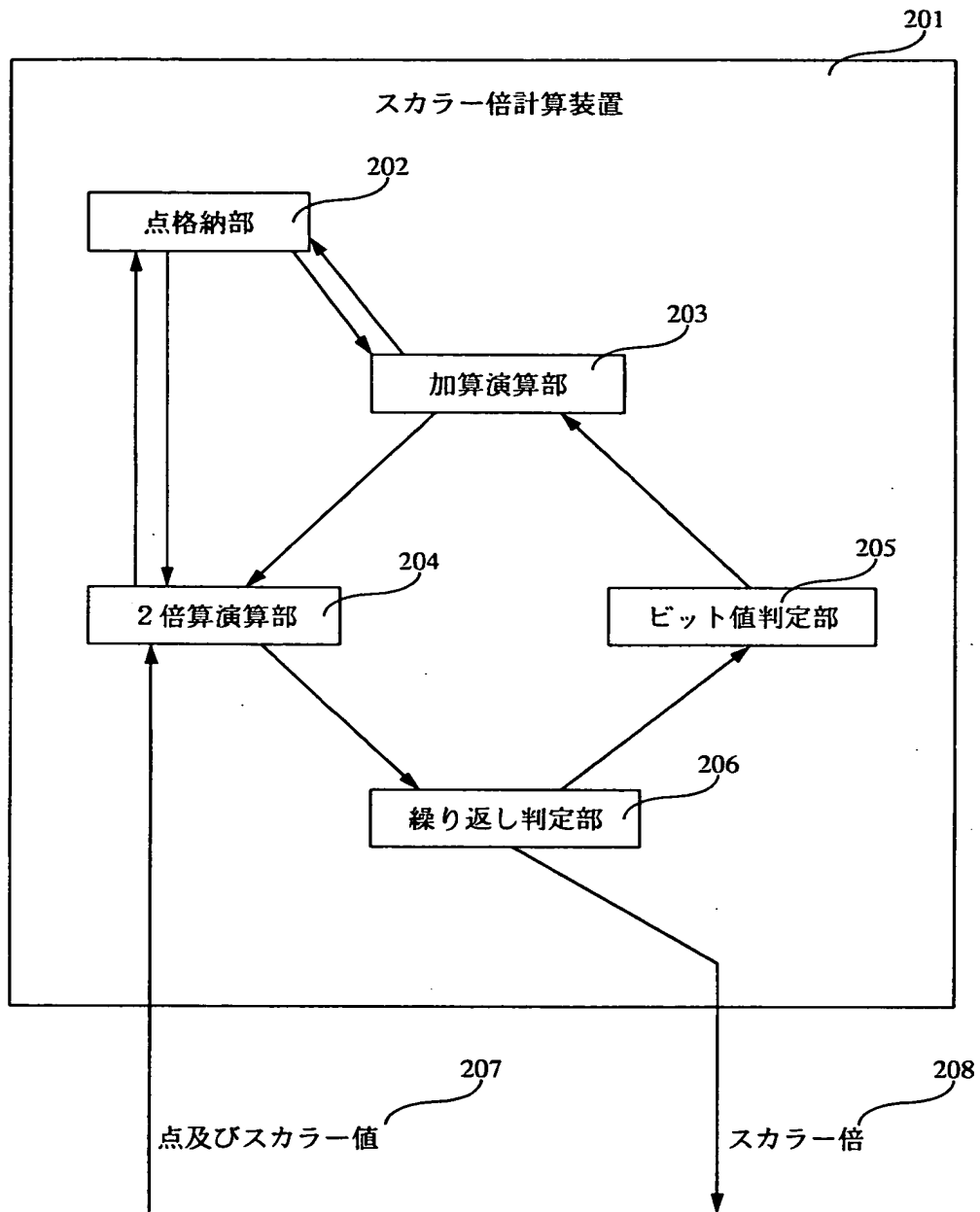
- 1 5 0 7 点及びスカラー値
- 1 5 0 8 スカラー倍
- 1 5 0 9 演算ランダム化部
- 2 7 0 1 スカラー倍計算装置
- 2 7 0 2 点格納部
- 2 7 0 3 加算演算部
- 2 7 0 4 2 倍算演算部
- 2 7 0 5 ビット値判定部
- 2 7 0 6 繰り返し判定部
- 2 7 0 7 点及びスカラー値
- 2 7 0 8 スカラー倍
- 2 7 0 9 ランダム化射影座標変換部
- 2 8 0 1 ランダム化射影座標変換装置
- 2 8 0 2 座標判定部
- 2 8 0 3 乱数生成部
- 2 8 0 4 射影座標変換部
- 2 8 0 5 楕円曲線上の点
- 2 8 0 6 ランダム化射影座標で表された点

【書類名】 図面

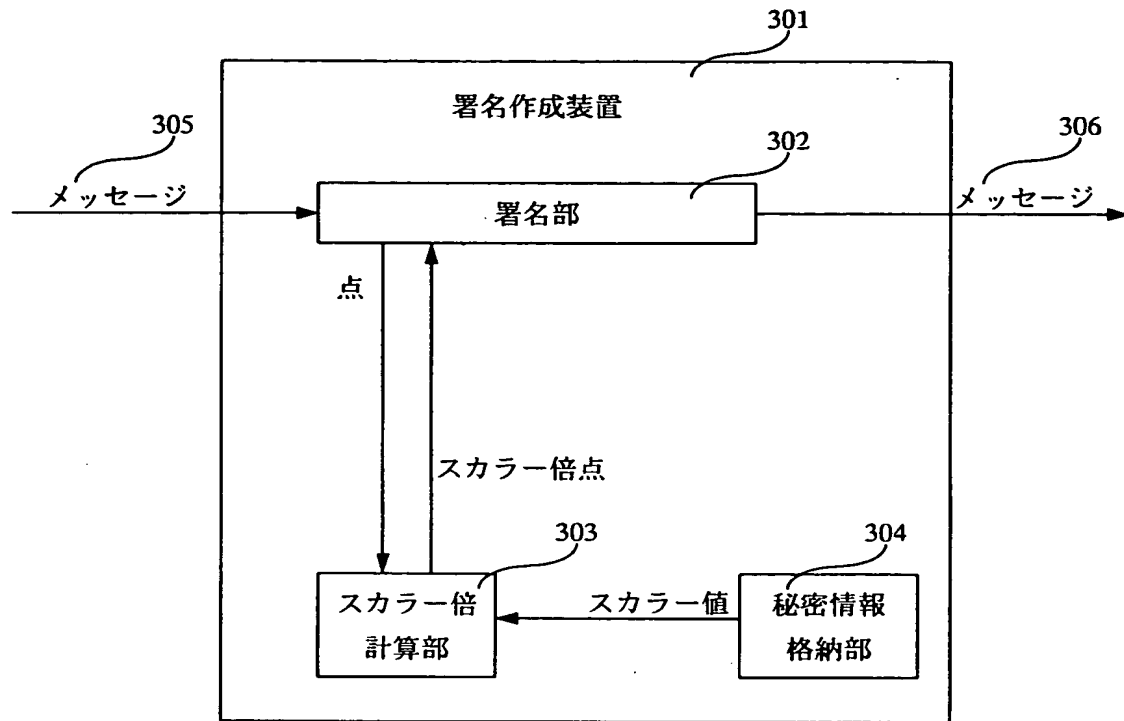
【図 1】



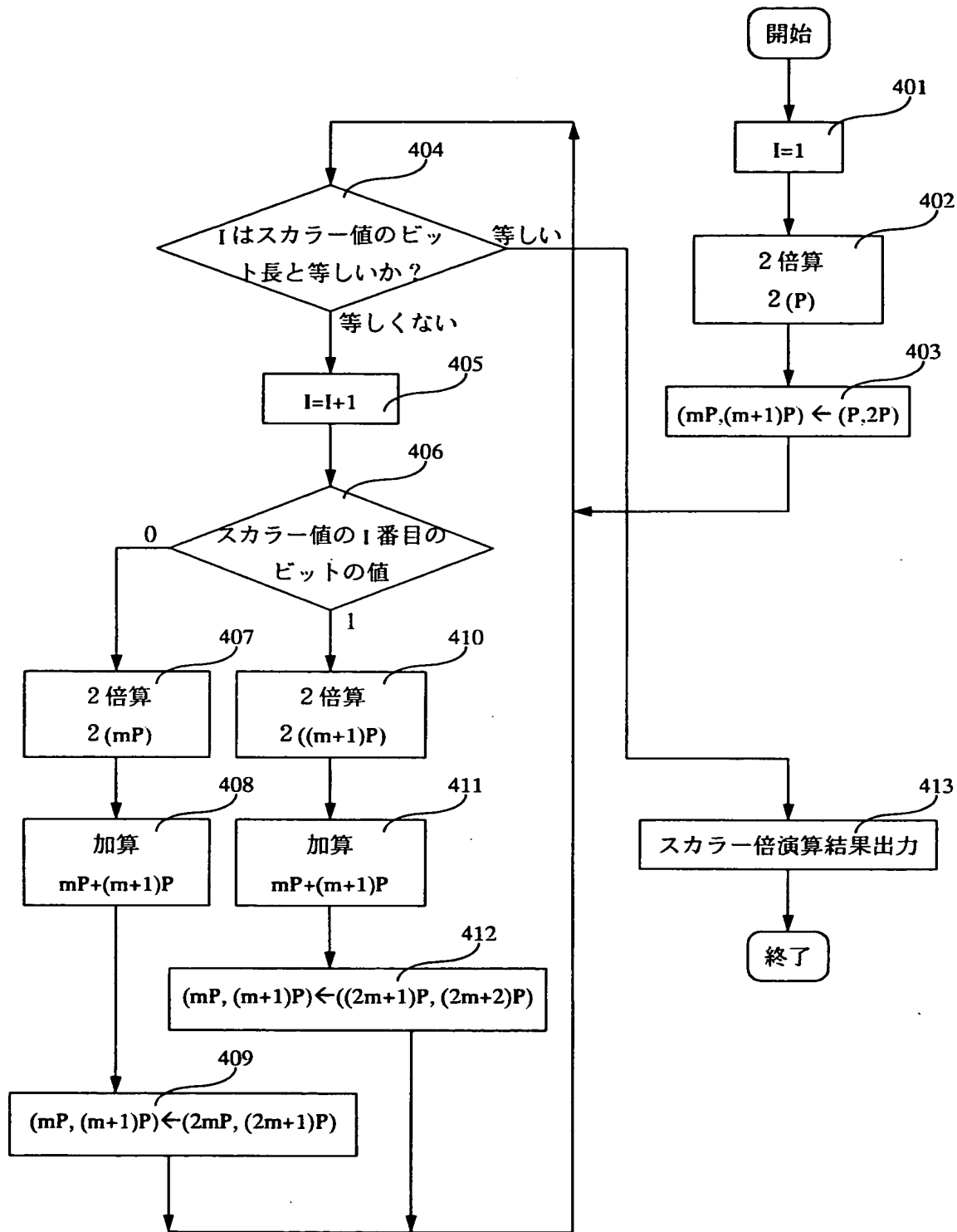
【図 2】



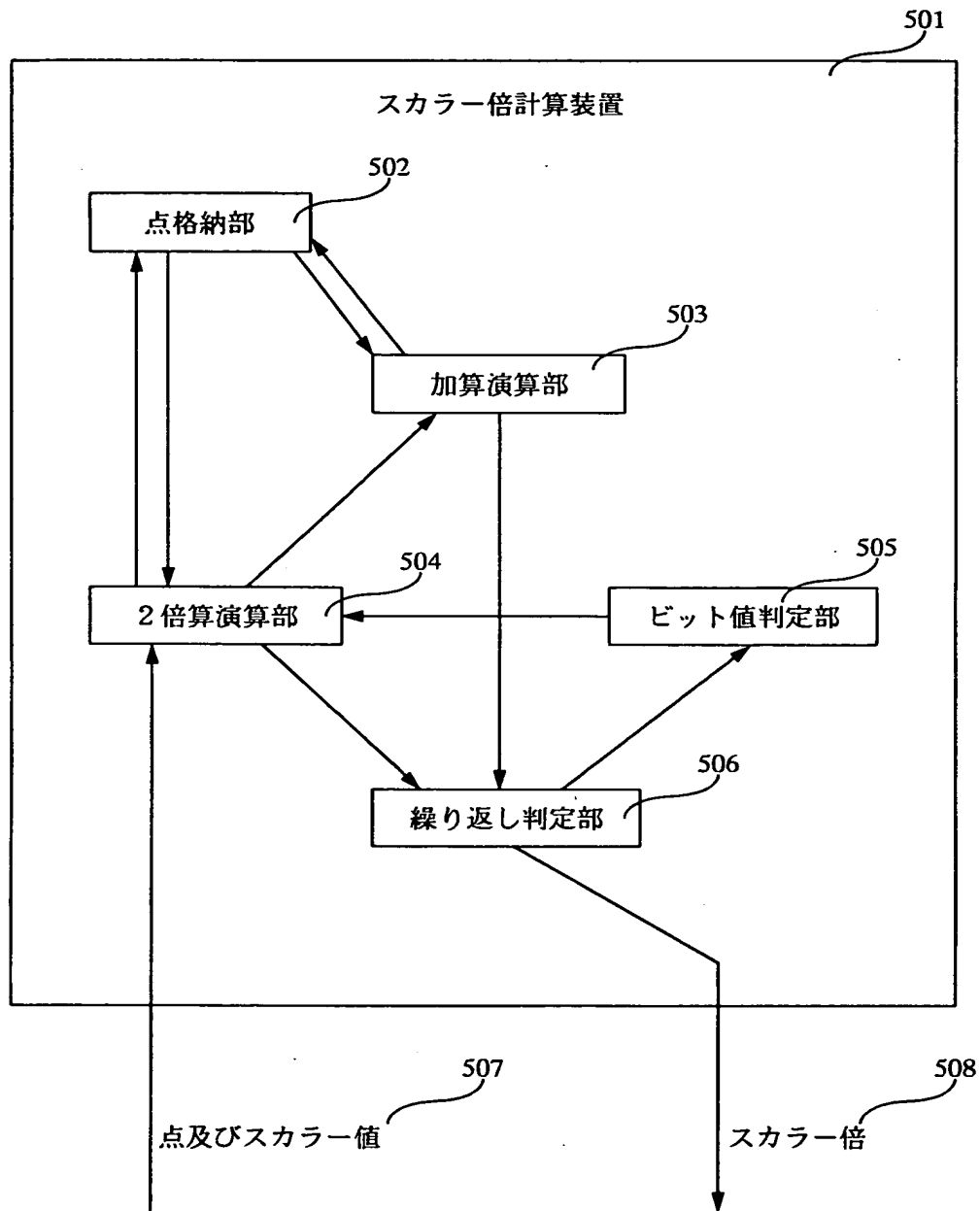
【図 3】



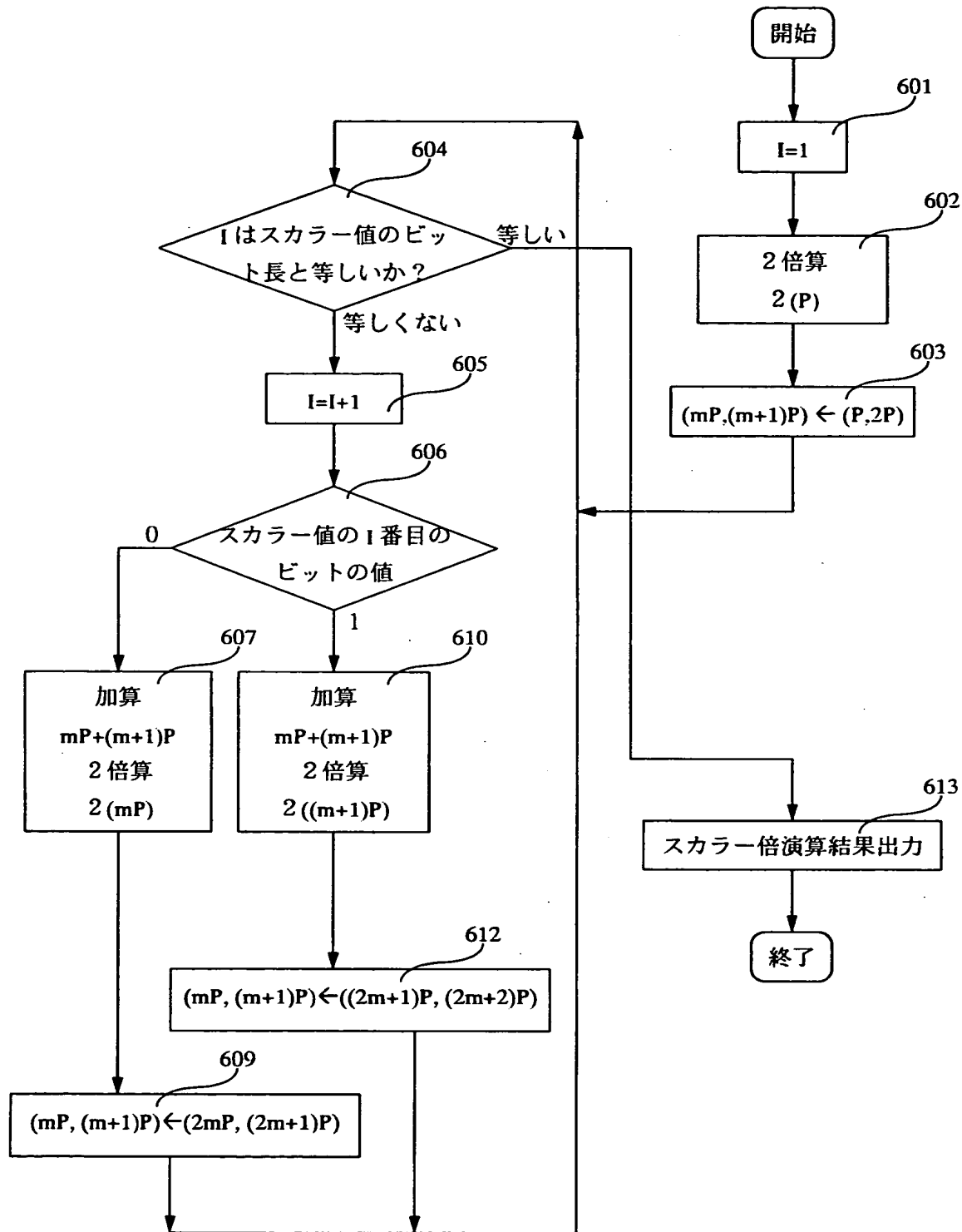
【図 4】



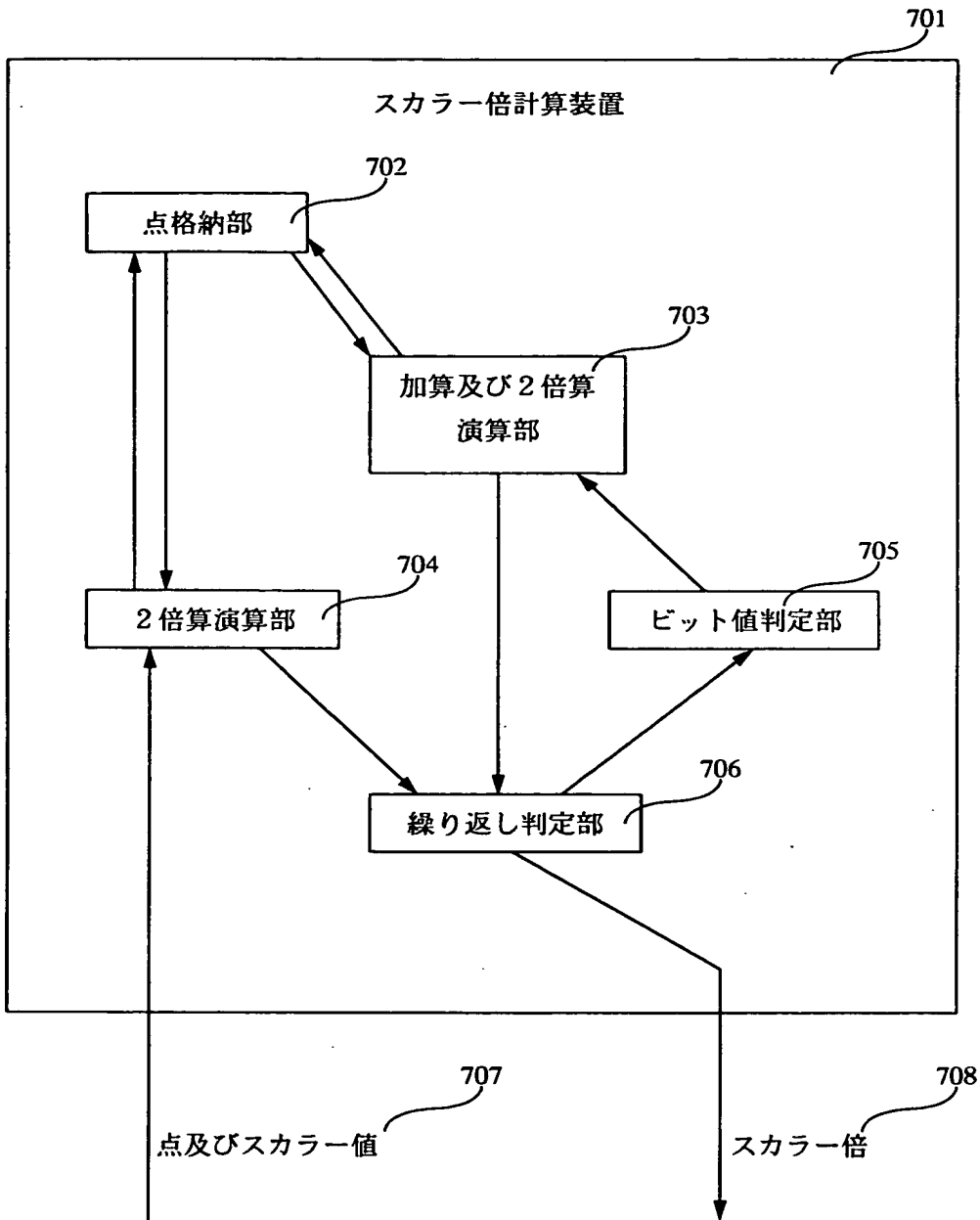
【図 5】



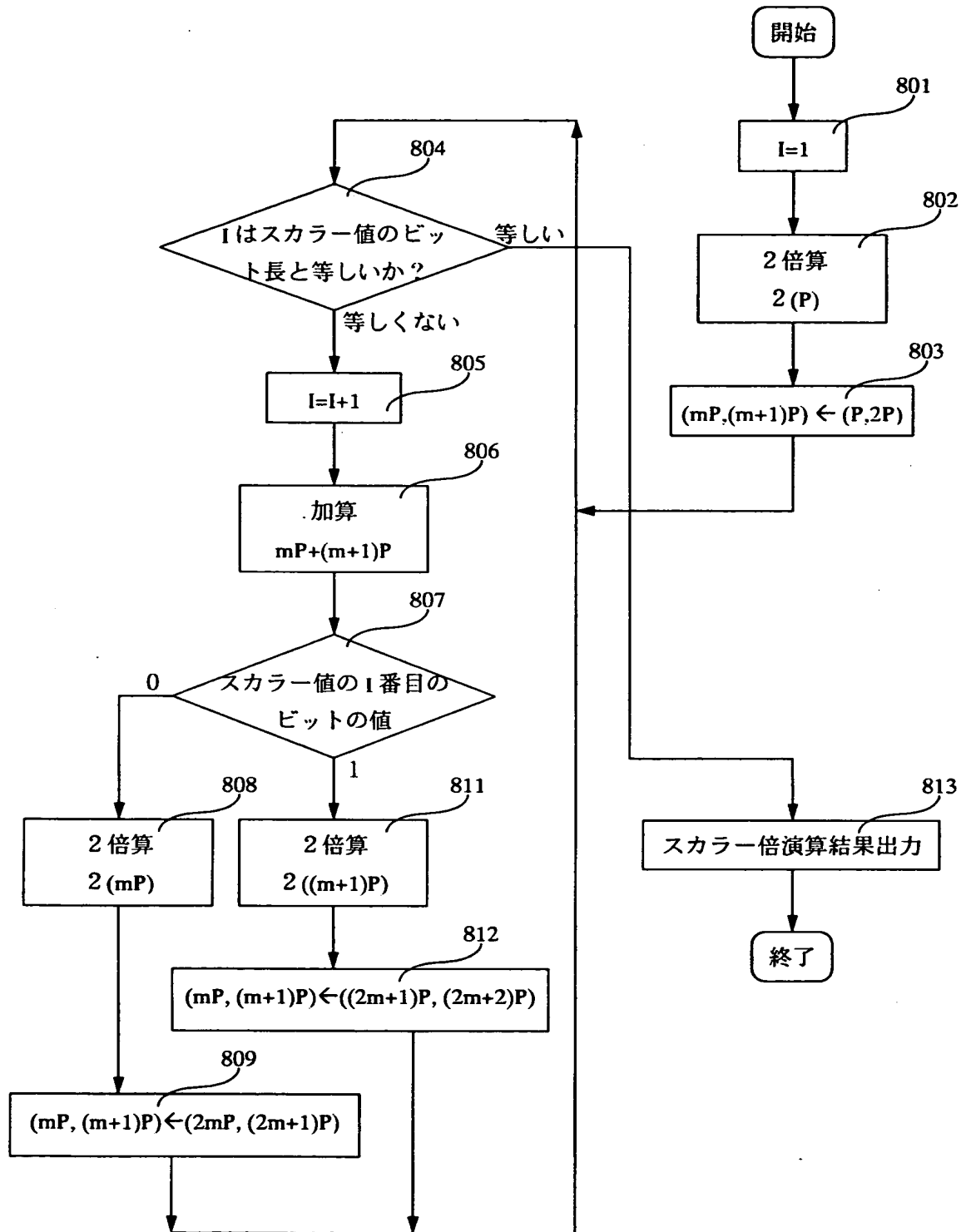
【図 6】



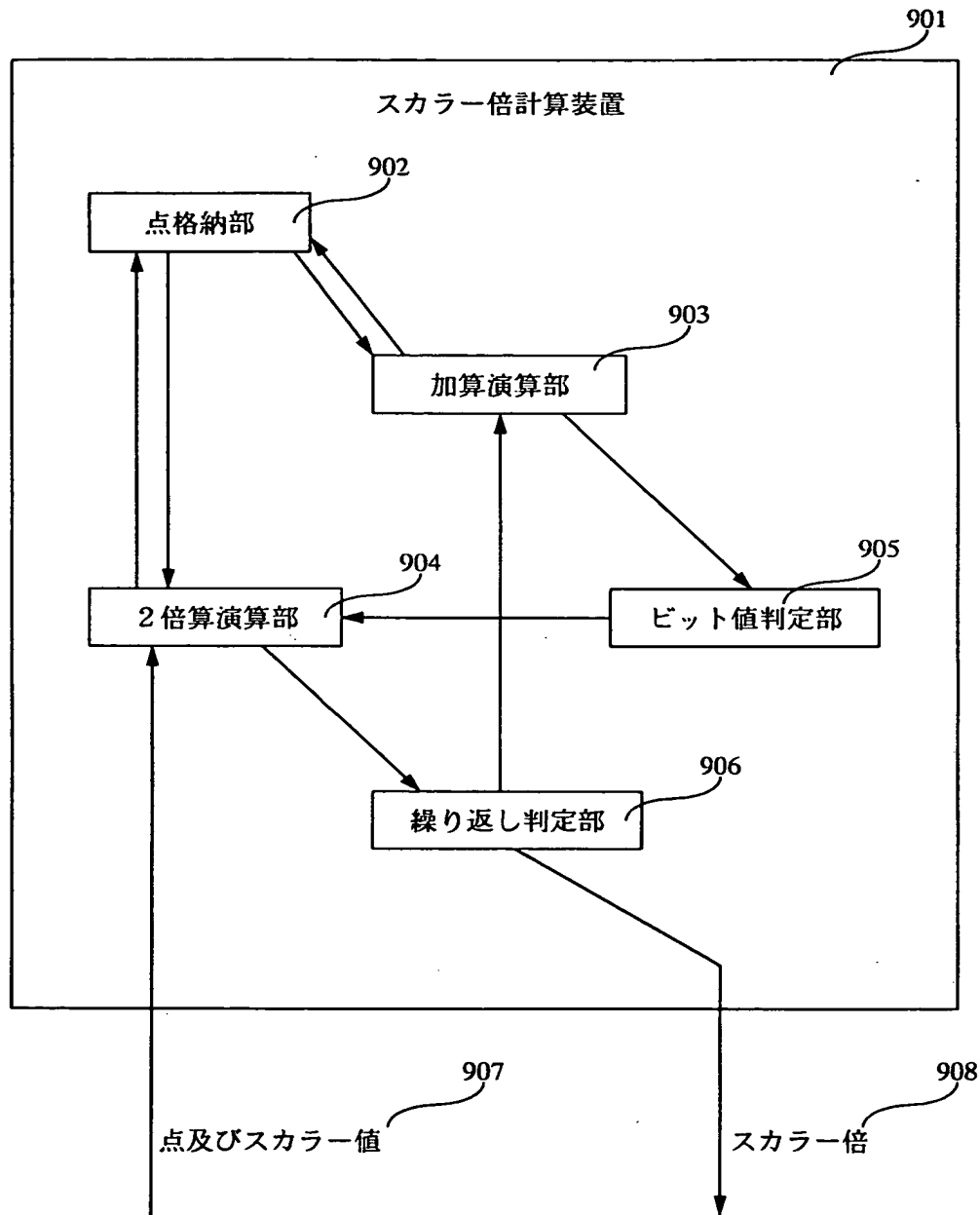
【図 7】



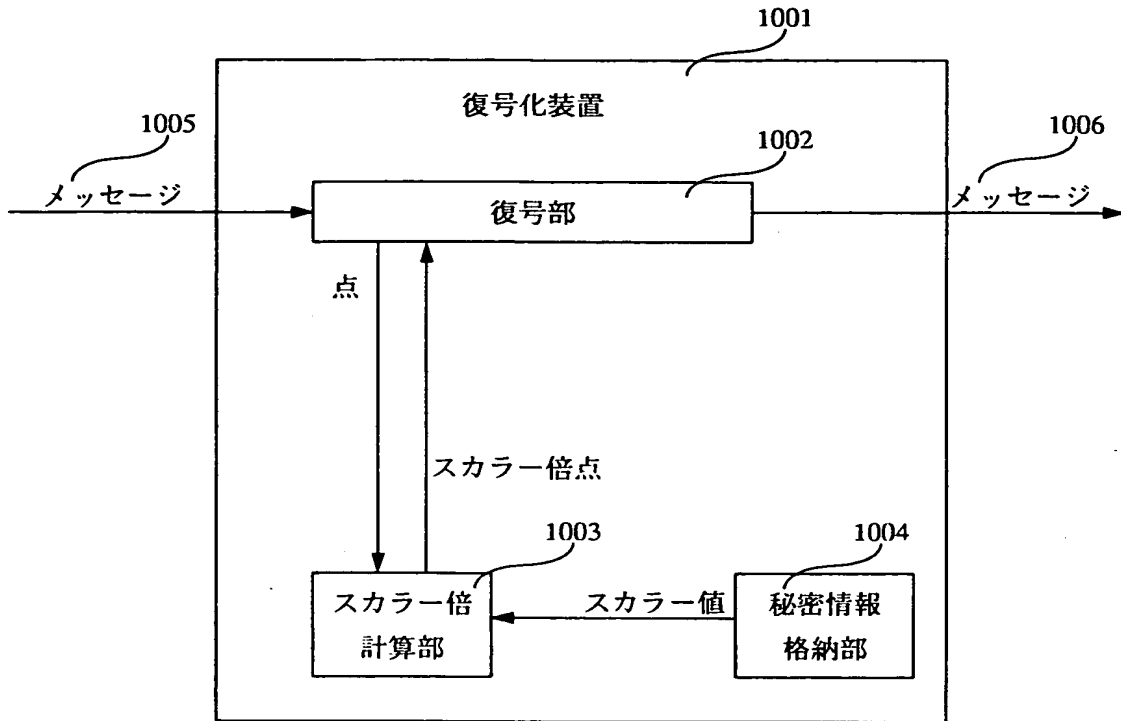
【図 8】



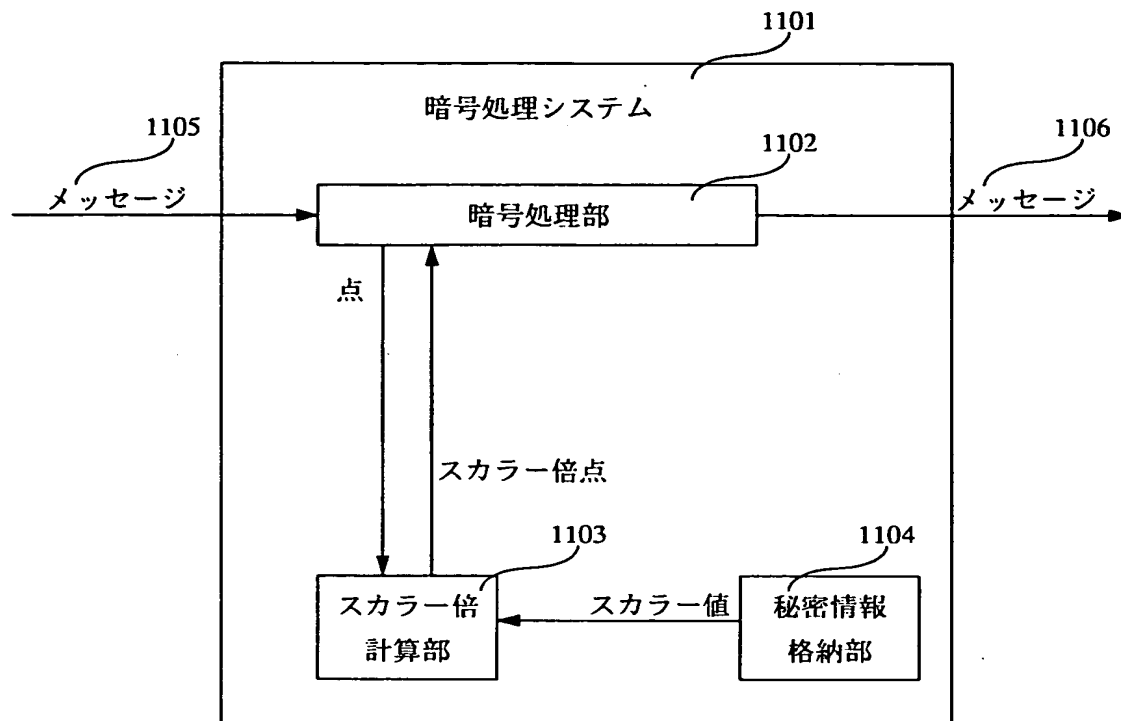
【図 9】



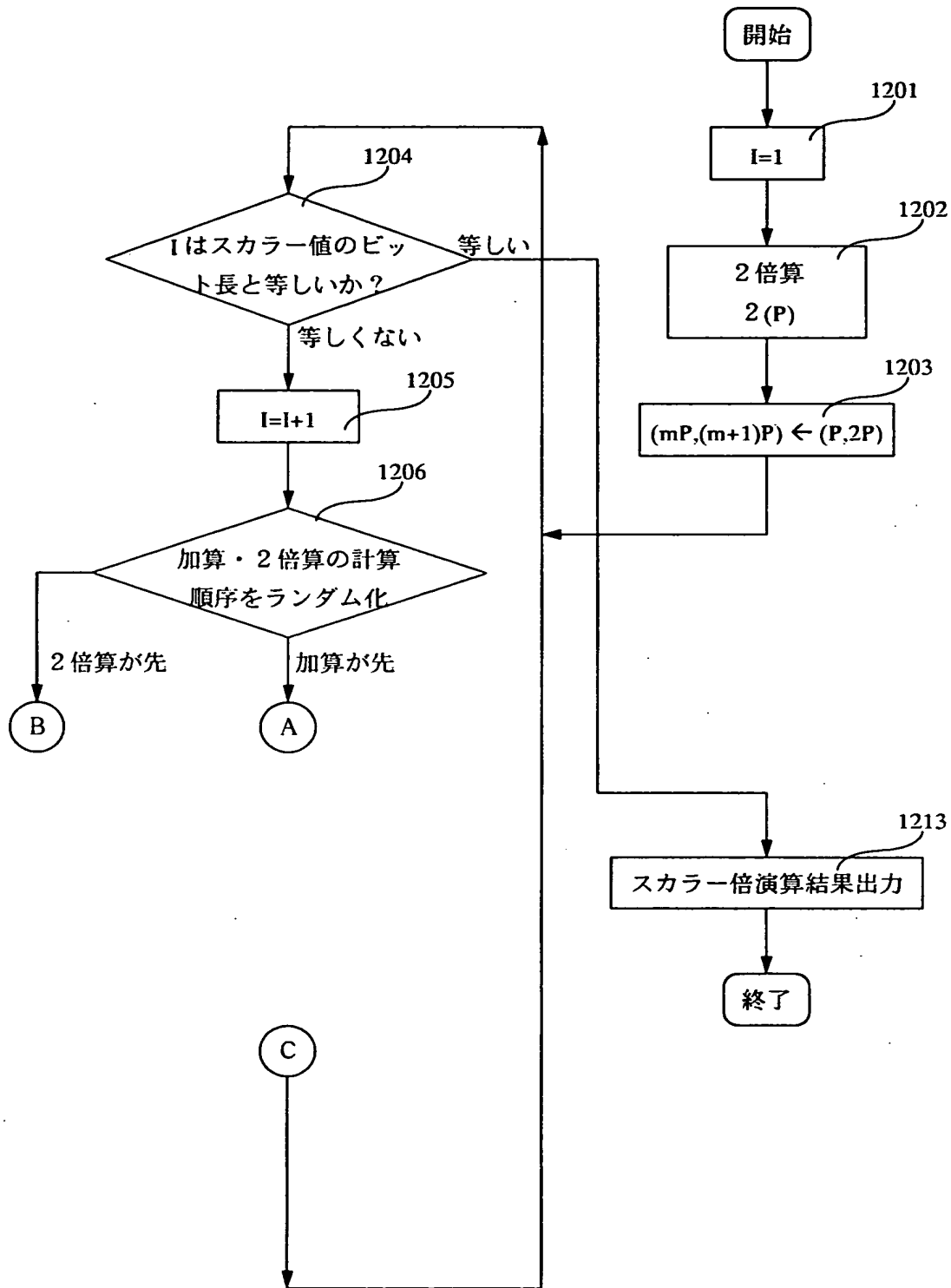
【図 1 0】



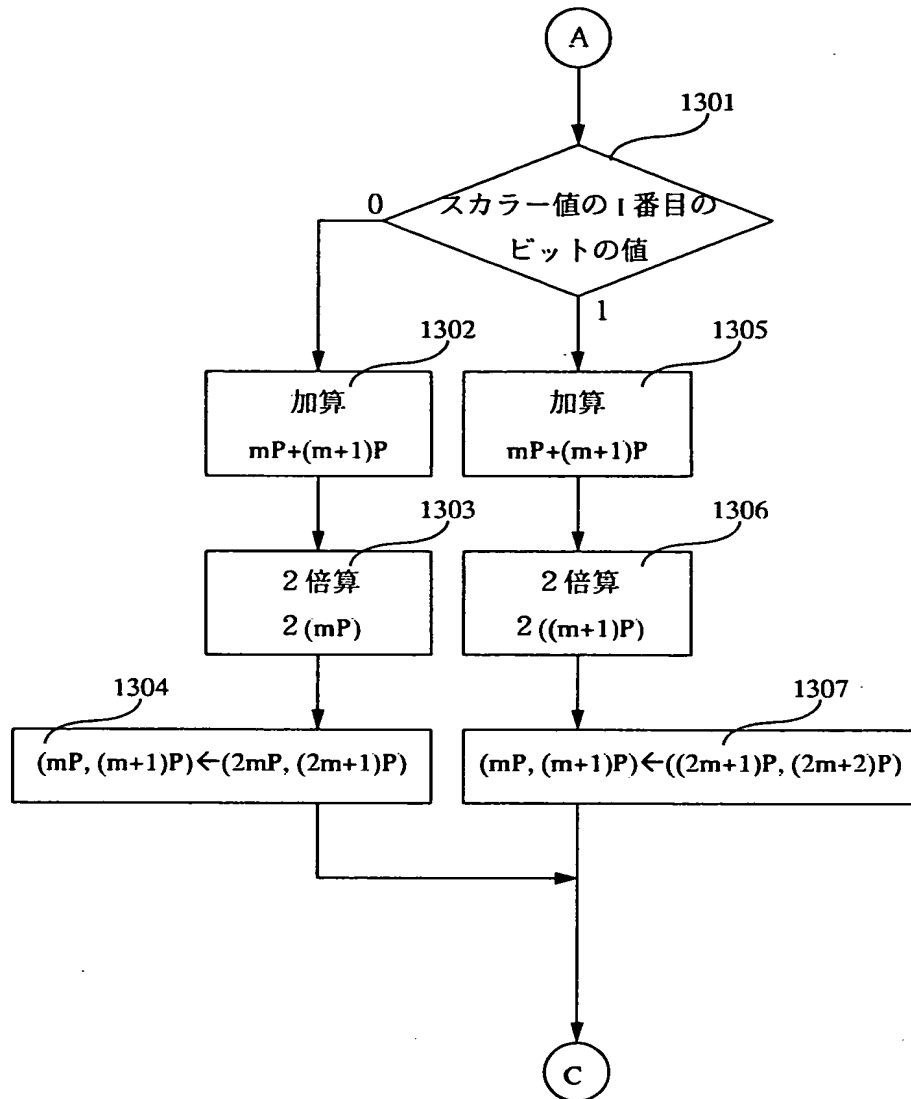
【図 1 1】



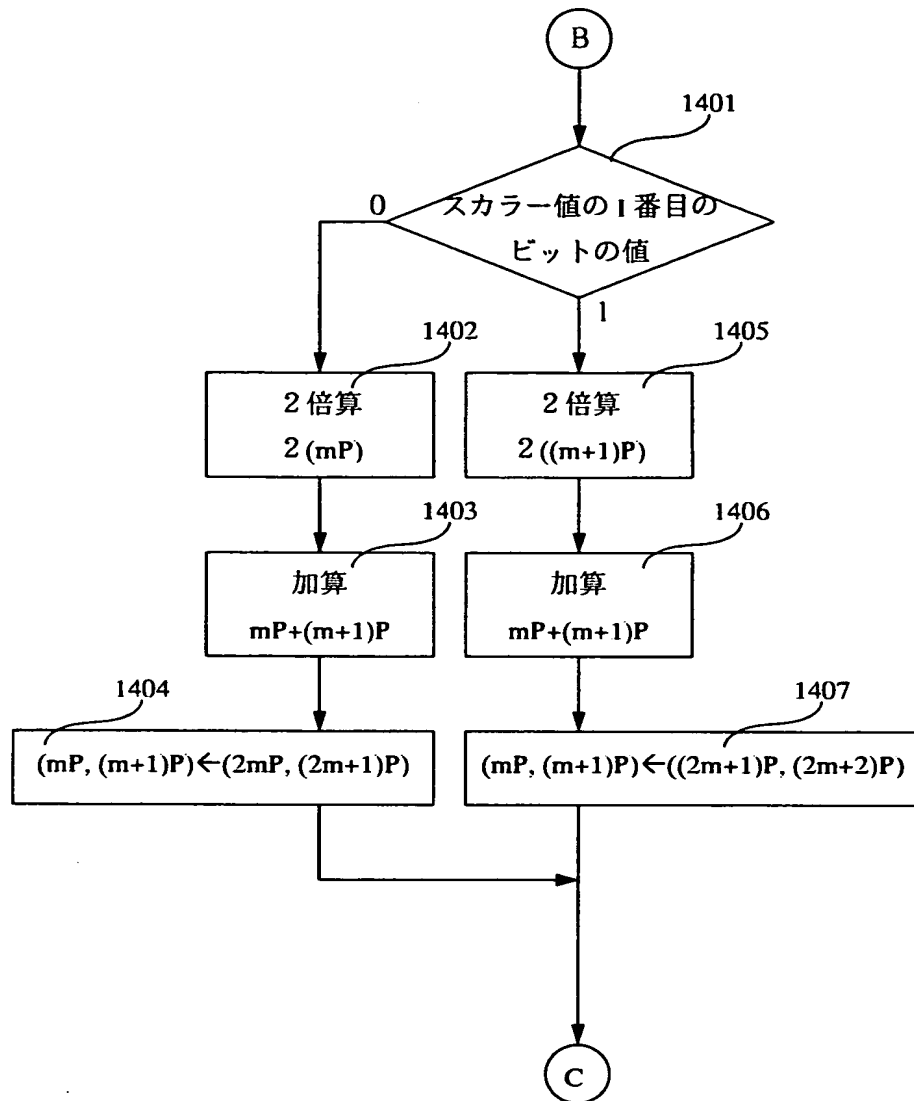
【図 12】



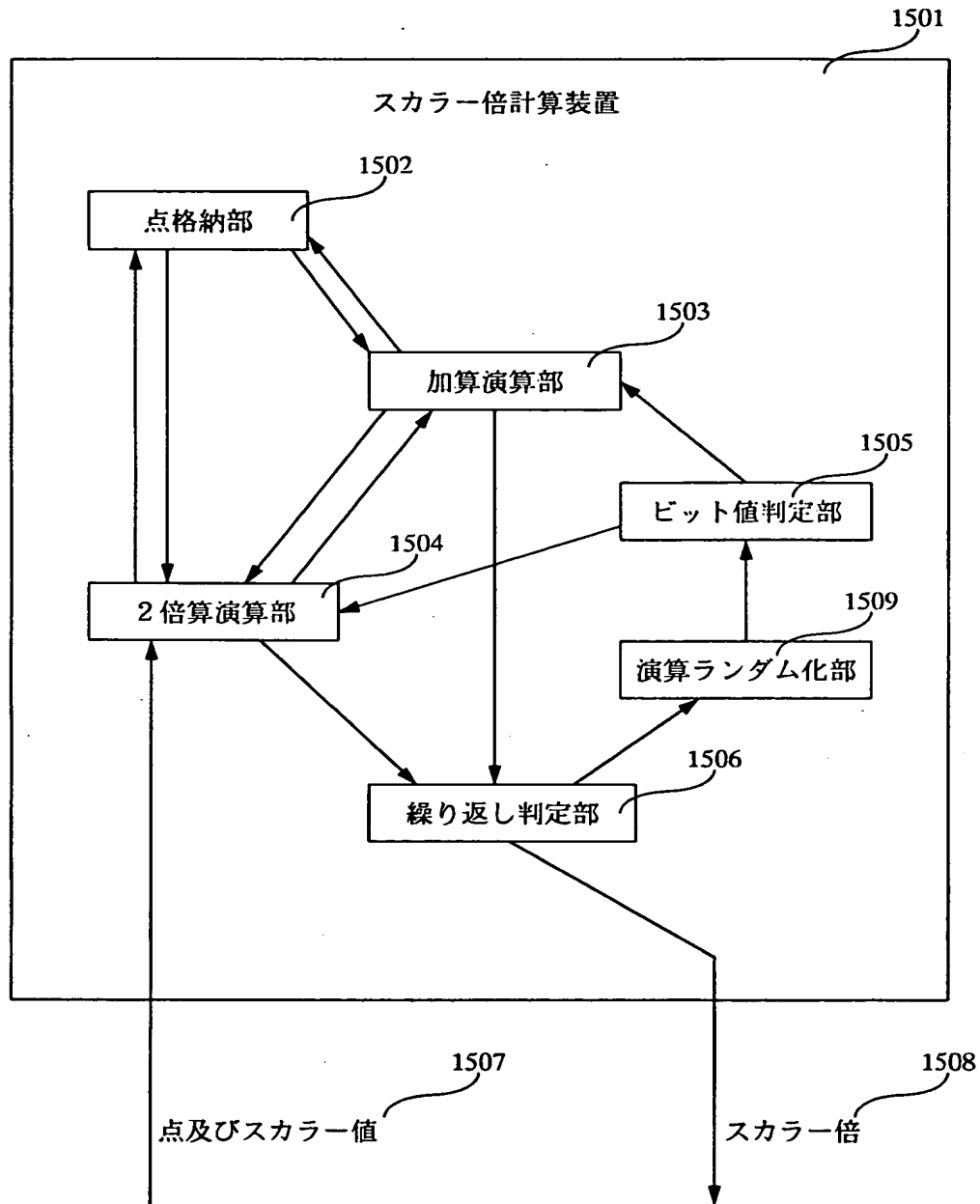
【図 1 3】



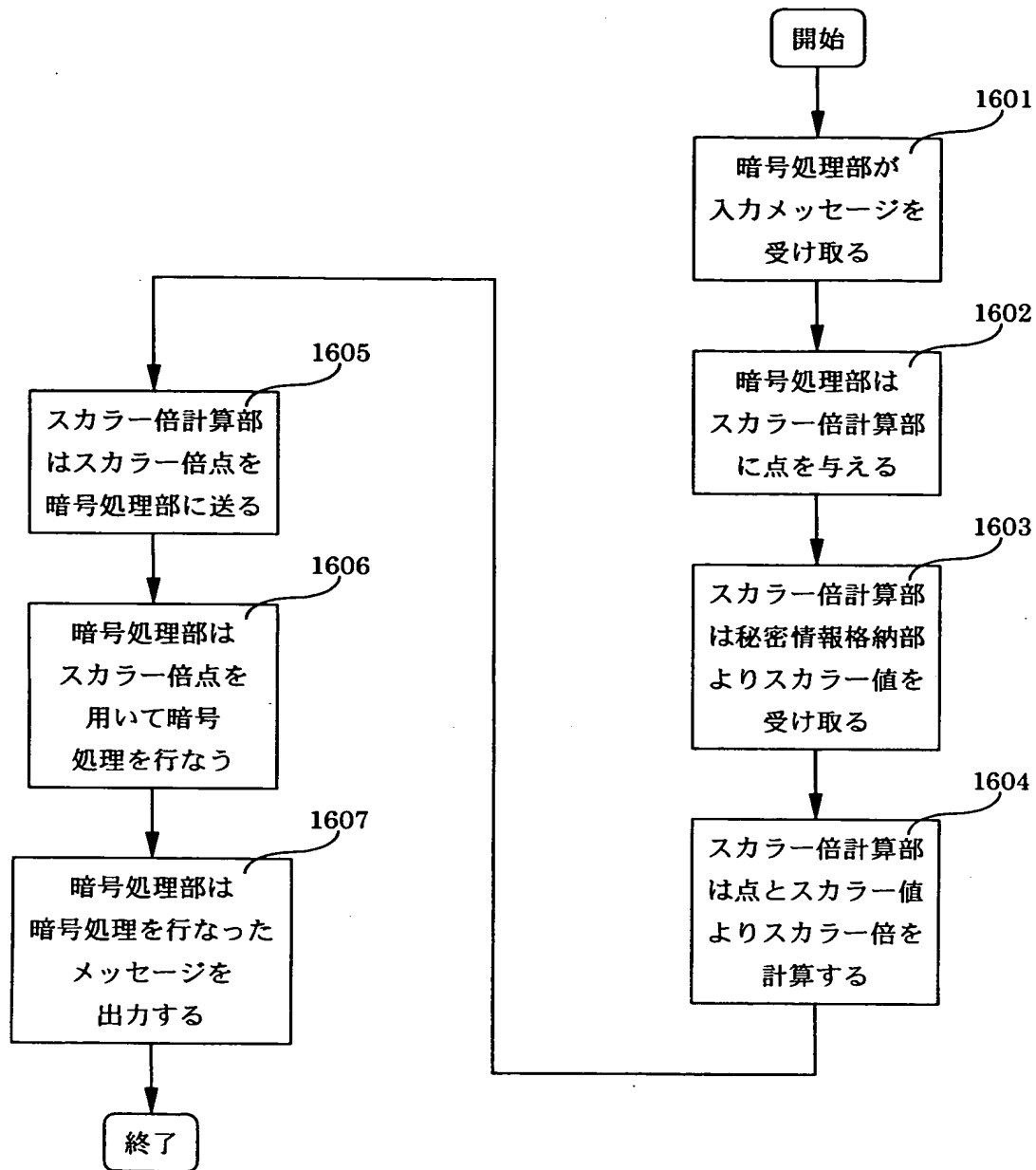
【図 1 4】



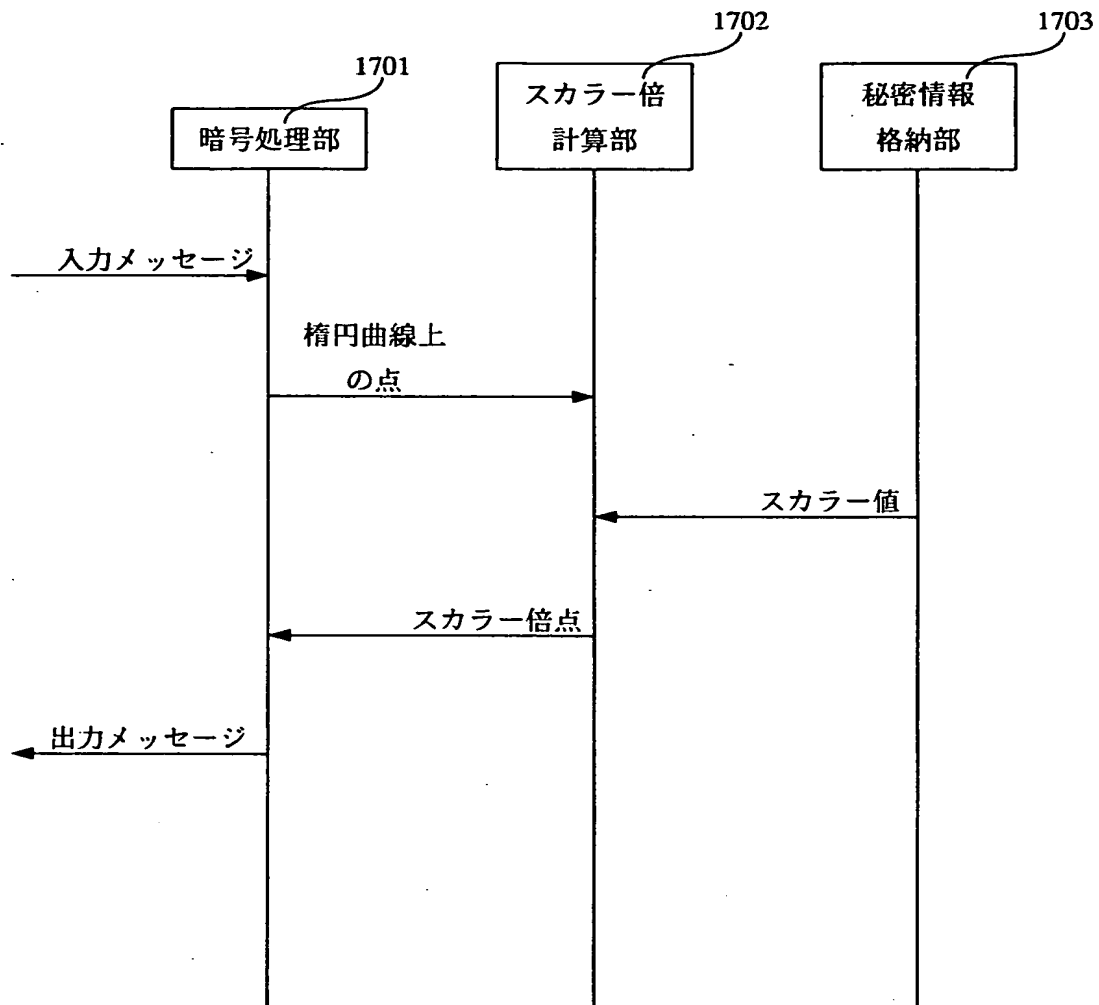
【図 1 5】



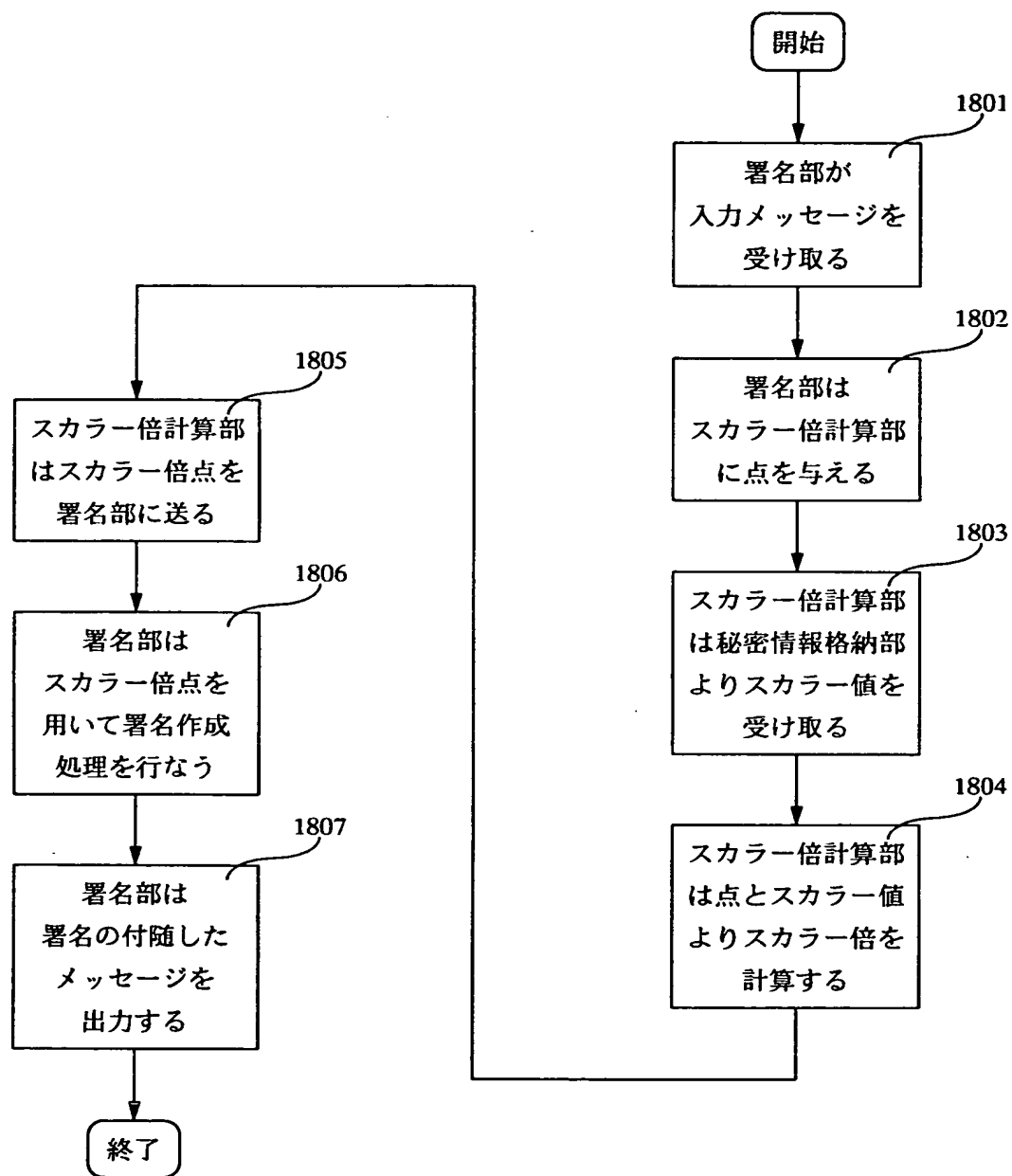
【図 1 6】



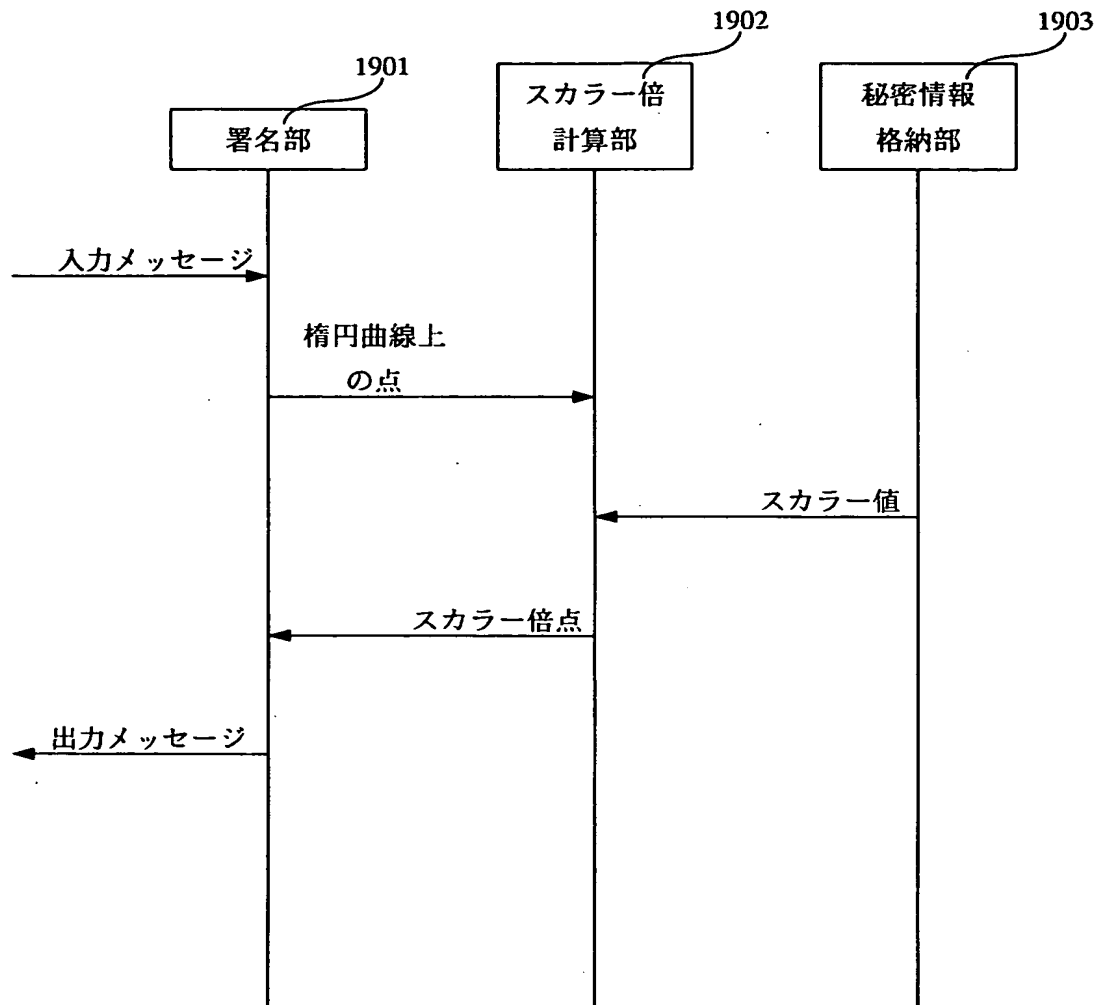
【図 1 7】



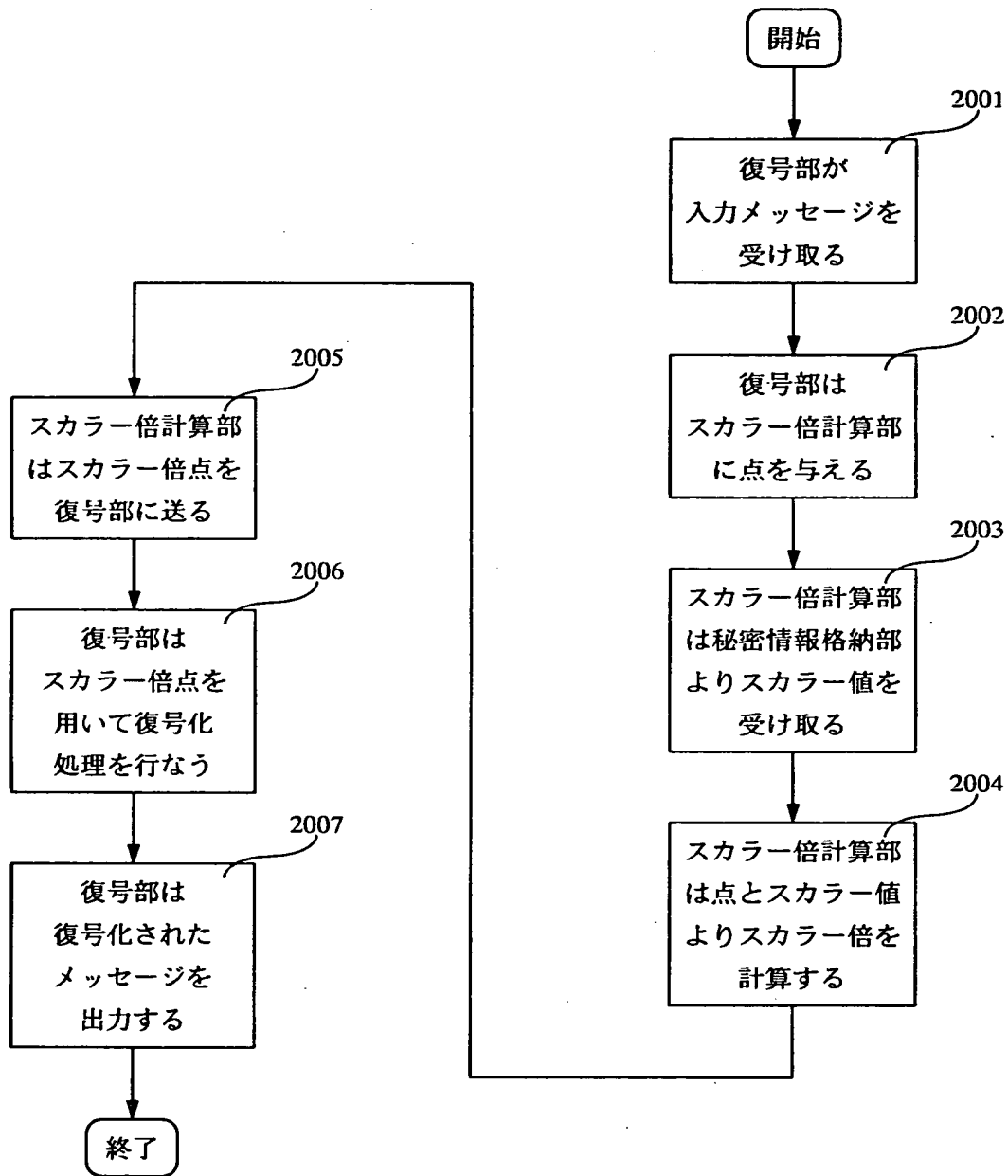
【図 1 8】



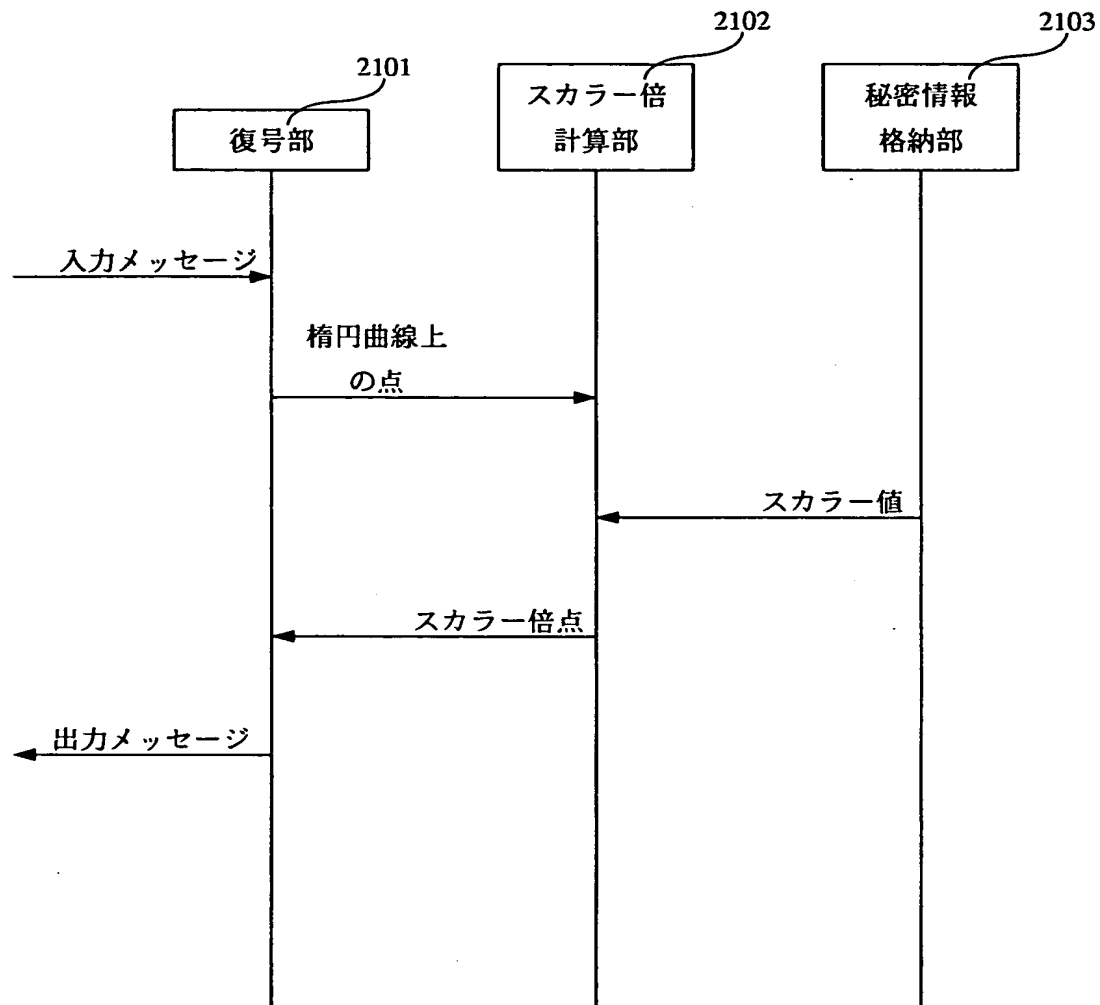
【図 1 9】



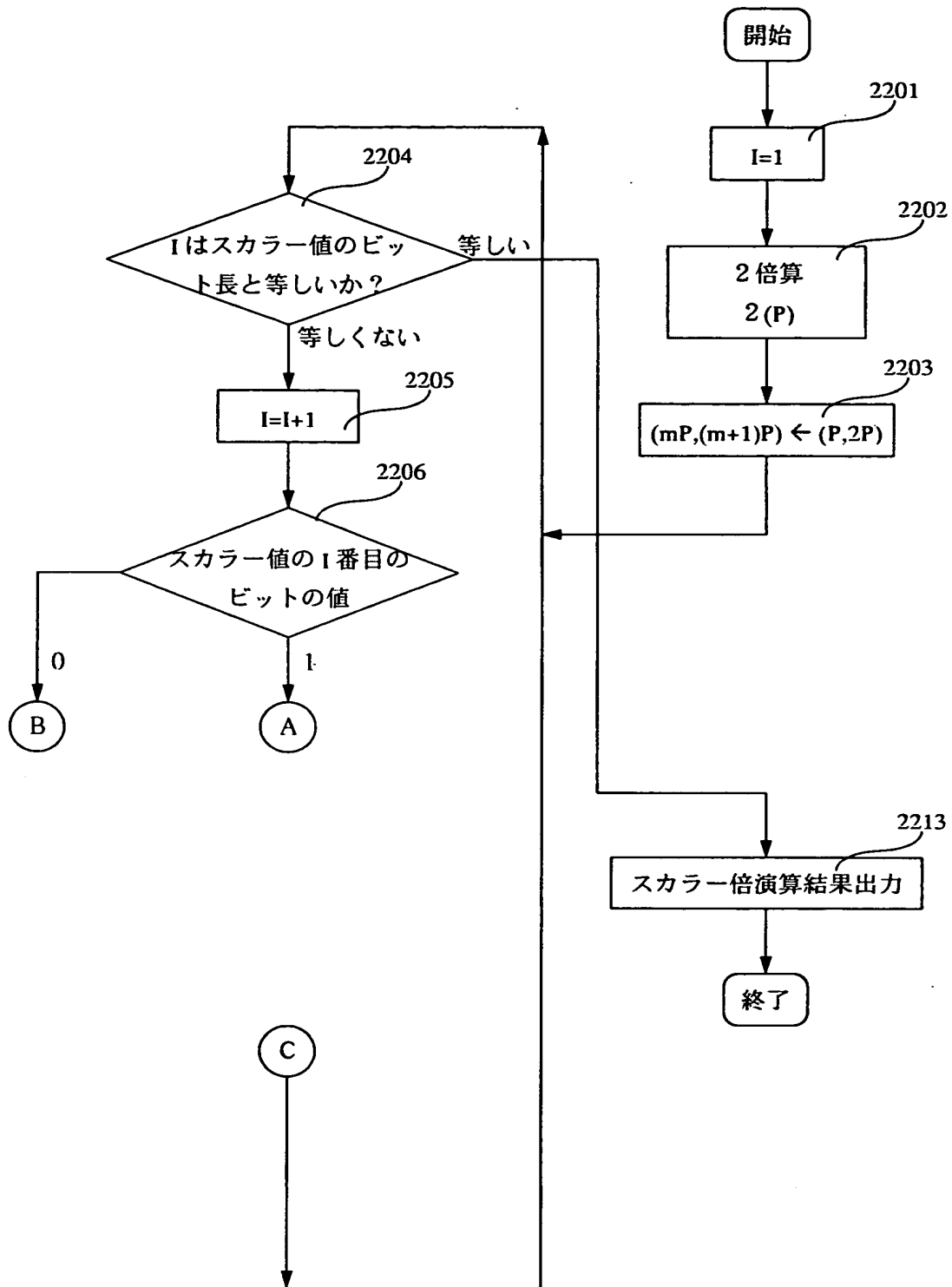
【図 2 0】



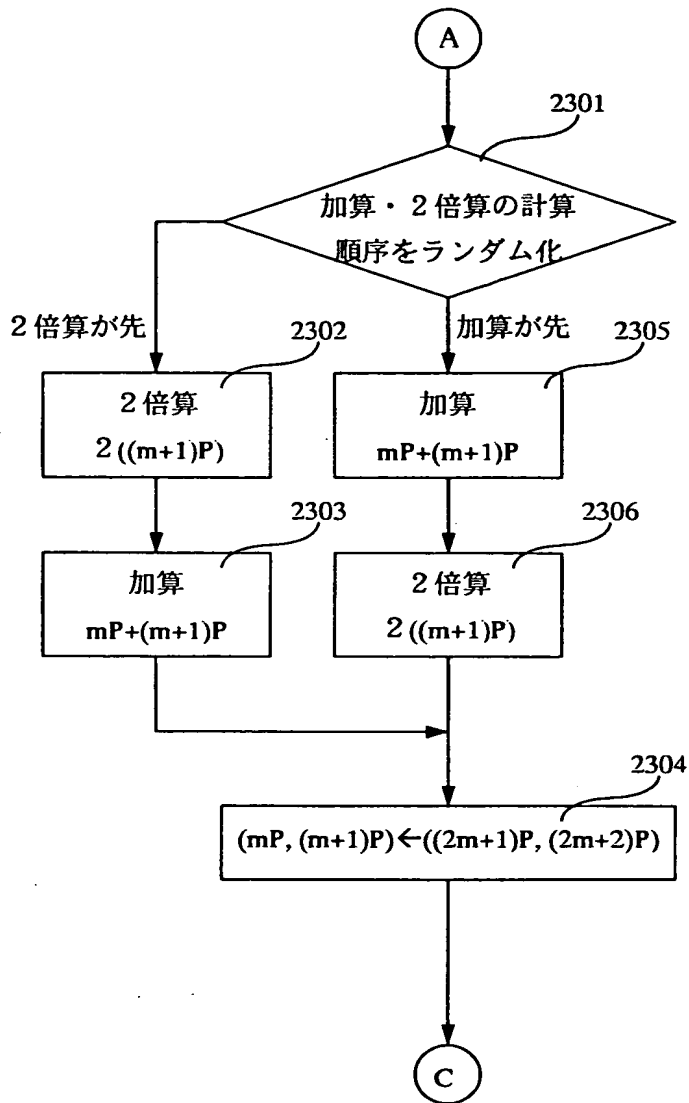
【図 2 1】



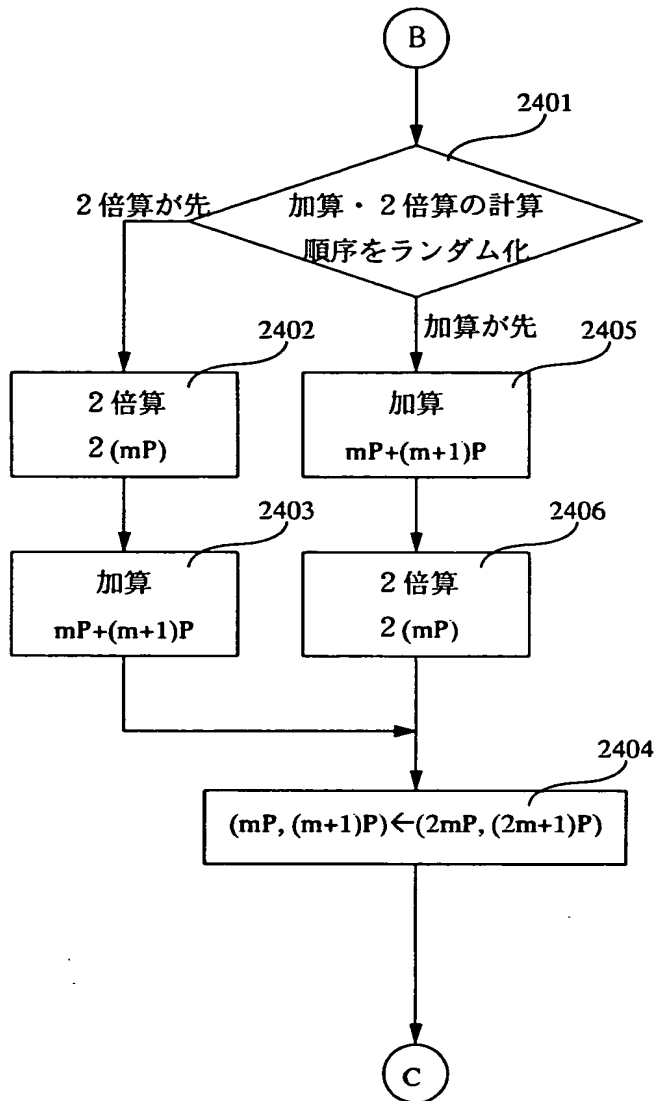
【図 22】



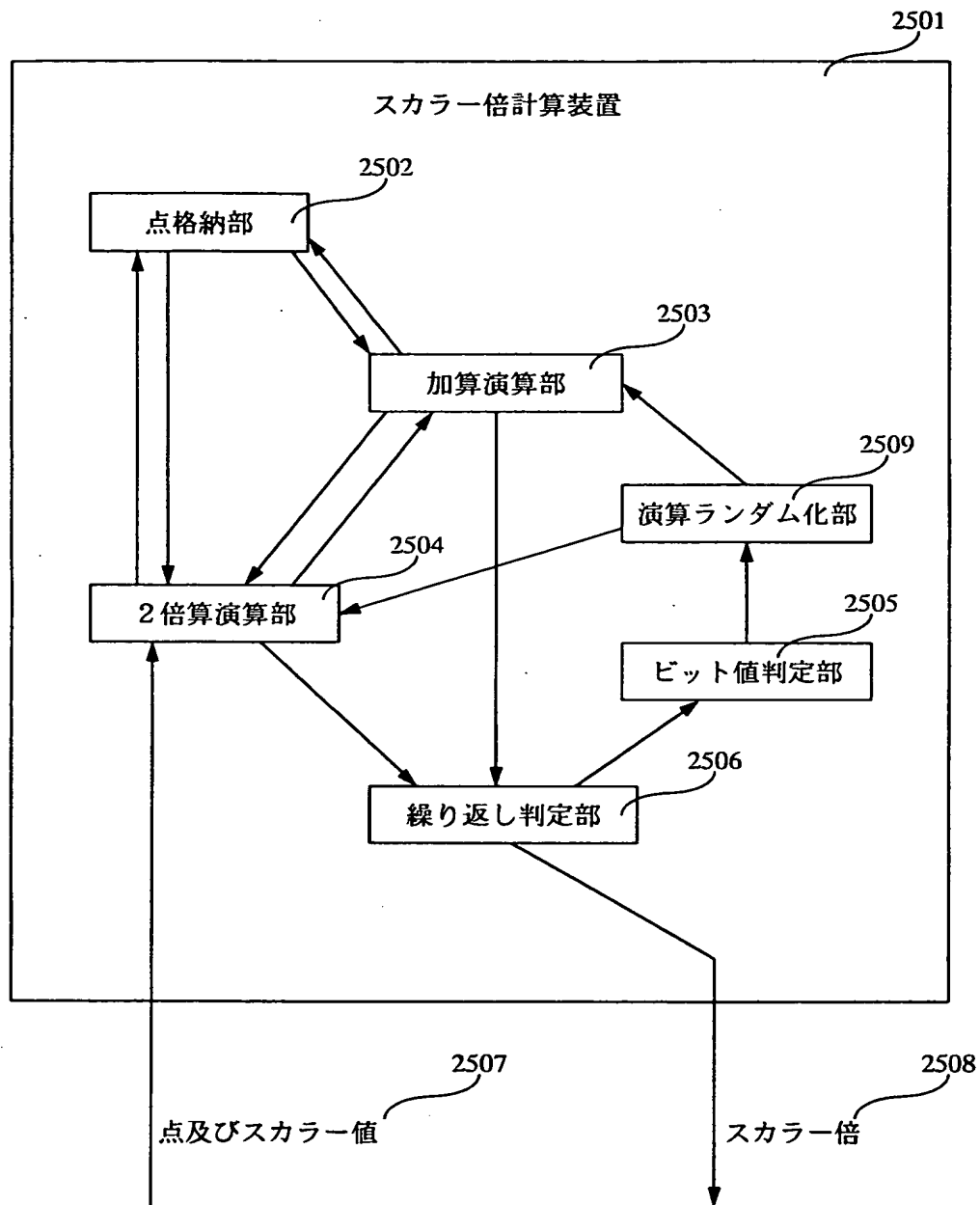
【図 2 3】



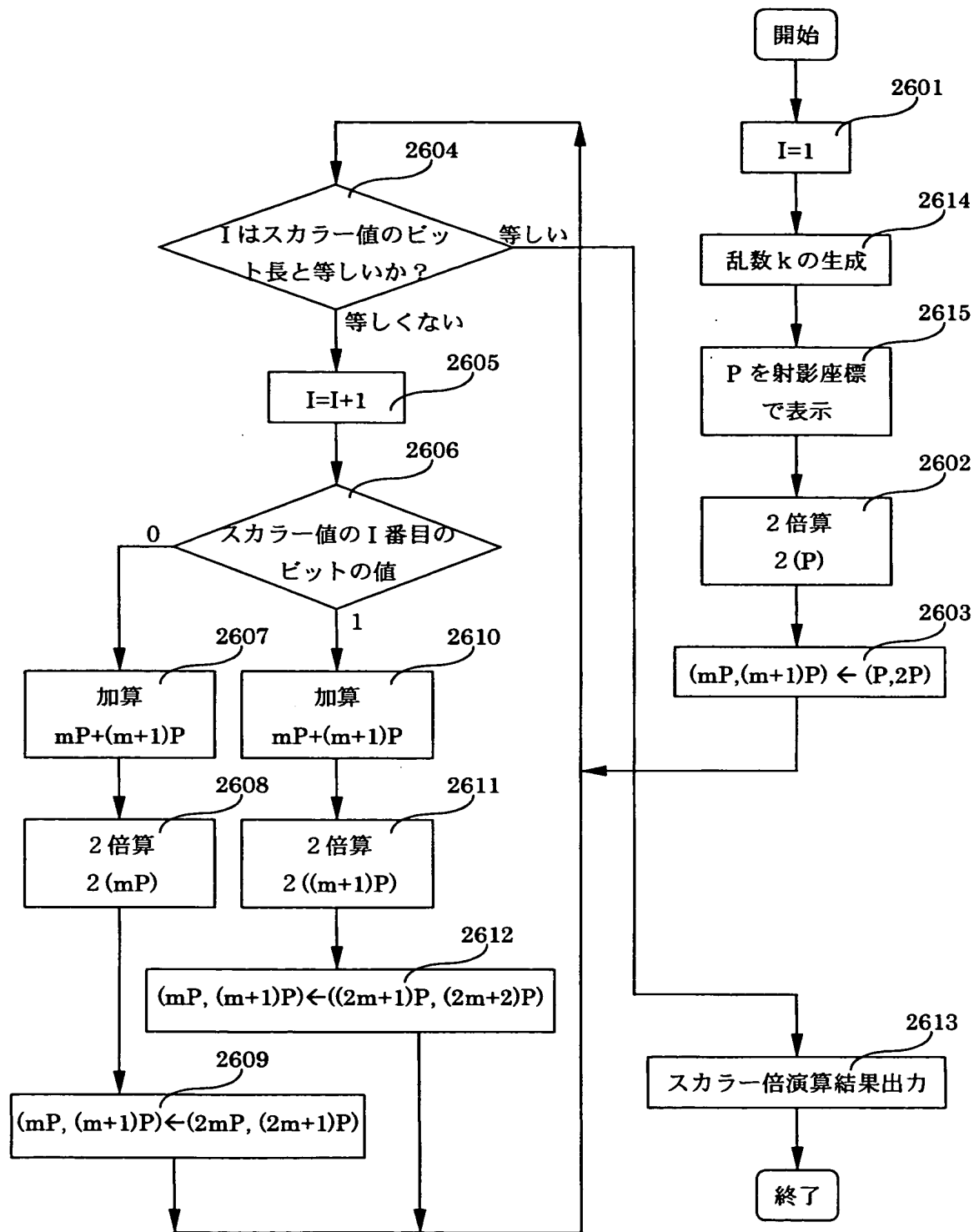
【図 2 4】



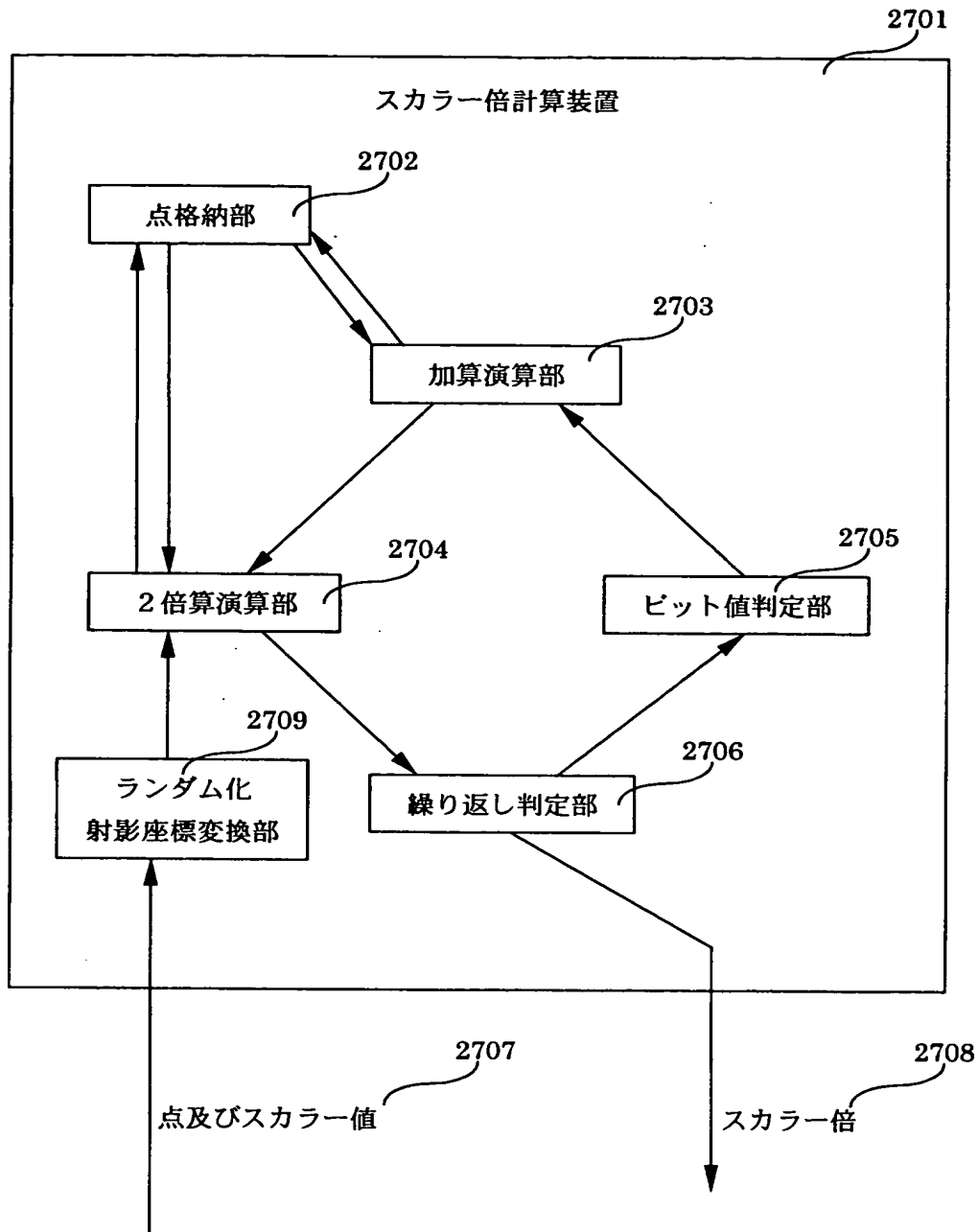
【図 2 5】



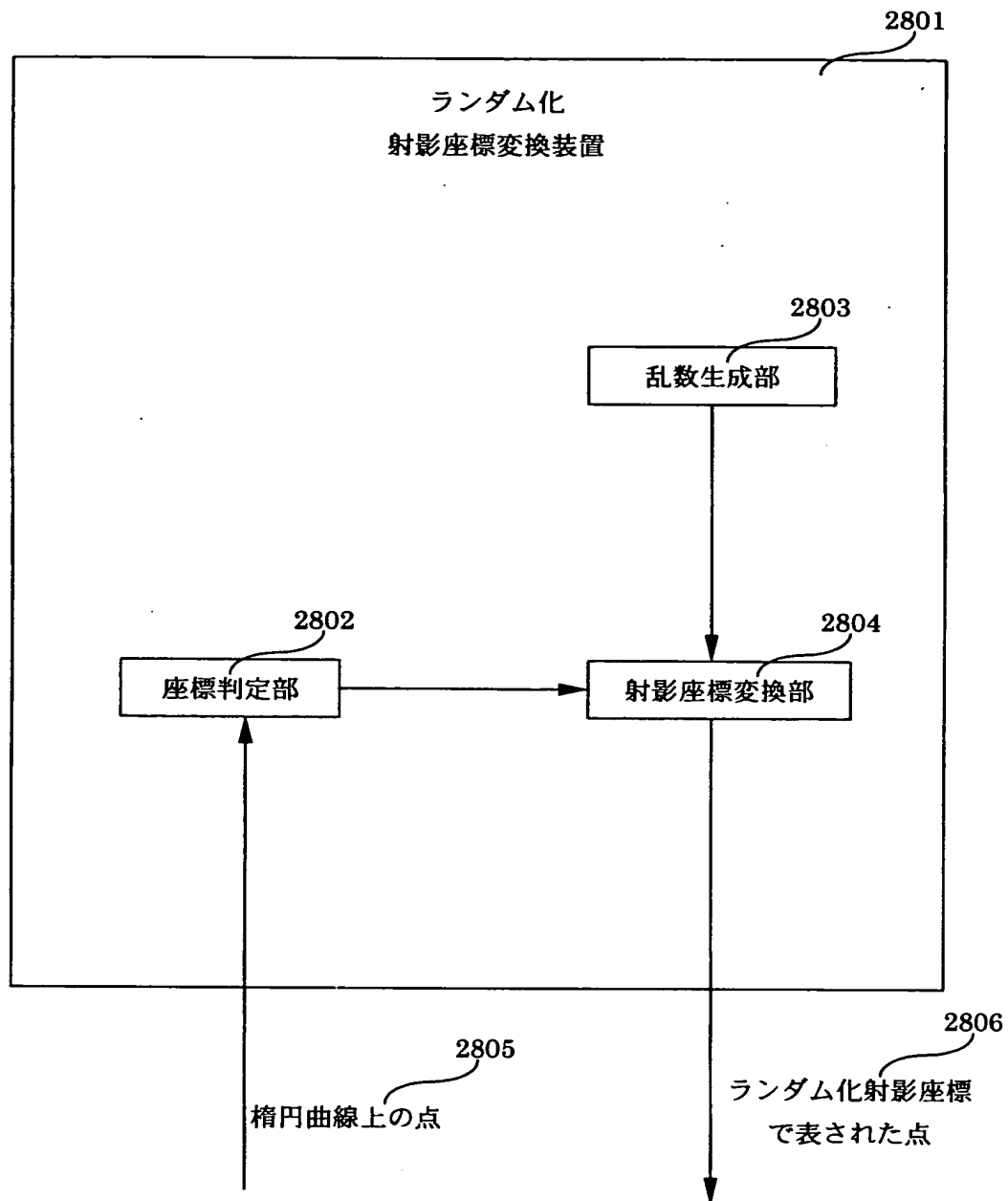
【図 26】



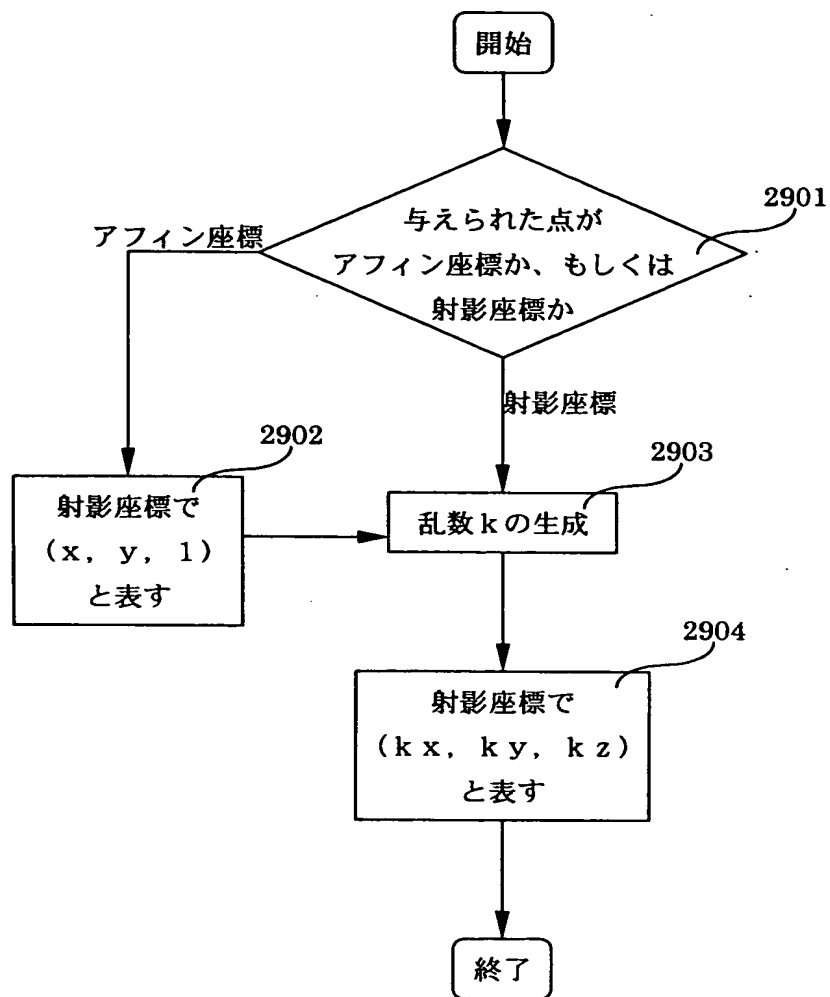
【図 2 7】



【図 2 8】



【図 29】



【書類名】 要約書

【要約】

【課題】

楕円曲線暗号における秘密情報を用いた暗号処理において、DPA等のパワーアナリシスという攻撃法により、暗号処理経過から秘密情報が復元される可能性があった。本発明の目的は、パワーアナリシスにより暗号処理経過が漏洩しても、秘密情報自体は漏洩せず、しかも高速に暗号処理を実行できる暗号処理方法を提供することにある。

【解決手段】

暗号処理経過と秘密情報との依存関係を断ち切った暗号処理方法を与える。特に、秘密情報であるスカラー値に対して、スカラー倍計算経過がそれらの値に依存しないスカラー倍計算方法を与える。すなわち、楕円曲線暗号においてスカラー値及び楕円曲線上の点からスカラー倍点を計算する際、スカラー値のビットの値を判定し、その判定を行なったビットの値に依存せずに一定の回数及び一定の順序で楕円曲線上の演算を実行する。

【選択図】 図2

認定・付加情報

特許出願の番号	特願2000-160001
受付番号	50000667141
書類名	特許願
担当官	第七担当上席 0096
作成日	平成12年 5月31日

<認定情報・付加情報>

【提出日】	平成12年 5月30日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日
[変更理由] 新規登録
住 所 東京都千代田区神田駿河台4丁目6番地
氏 名 株式会社日立製作所

く。

【0070】

ステップ1302として、加算演算部1503により、点格納部1502に格納されている点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ1303へ行く。ステップ1303として、2倍算演算部1504により、点格納部1502に格納されている点の組 $(mP, (m+1)P)$ から点 mP の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ1304へ行く。ステップ1304として、ステップ1303で求めた点 $2mP$ とステップ1302で求めた点 $(2m+1)P$ を点格納部1502に点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ1204へ戻る。

【0071】

ステップ1305として、加算演算部1503により、点格納部1502に格納されている点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ1306へ行く。ステップ1306として、2倍算演算部1504により、点格納部1502に格納されている点の組 $(mP, (m+1)P)$ から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ1307へ行く。ステップ1307として、ステップ1305で求めた点 $(2m+1)P$ とステップ1306で求めた点 $(2m+2)P$ を点格納部1502に点の組 $((2m+1)P, (2m+2)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ1204へ戻る。

【0072】

ステップ1401として、ビット値判定部1505により、スカラー値の I 番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ1402へ行く。そのビットの値が1であればステップ1405へ行く。

【0073】

ステップ1402として、2倍算演算部1504により、点格納部1502に格納されている点の組 $(mP, (m+1)P)$ から点 mP の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ1403へ行く。ステップ1403として、加算演算部1503により、点格納部1502に格納されている点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ1404へ行く。ステップ1404として、ステップ1402で求めた点 $2mP$ とステップ1403で求めた点 $(2m+1)P$ を点格納部1502に点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ1204へ戻る。

【0074】

ステップ1405として、2倍算演算部1504により、点格納部1502に格納されている点の組 $(mP, (m+1)P)$ から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ1406へ行く。ステップ1406として、加算演算部1503により、点格納部1502に格納されている点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ1407へ行く。ステップ1407として、ステップ1406で求めた点 $(2m+1)P$ とステップ1405で求めた点 $(2m+2)P$ を点格納部1502に点の組 $((2m+1)P, (2m+2)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ1204へ戻る。

【0075】

ステップ1213として、点格納部1502に格納されている点の組 $(mP, (m+1)P)$ から、点 mP をスカラー倍1508として出力し、終了する。

【0076】

以上の手順により出力する値である点 mP が点 P のスカラー値 d によるスカラー倍の点 dP となることは、第1実施例の場合と同様に示すことができる。

【0077】

また、楕円曲線としてモンゴメリ型楕円曲線を用いると、加算及び2倍算が高

速に実行可能であり、通常用いる標準型楕円曲線よりも高速にスカラー倍計算が実行可能である。

【 0 0 7 8 】

標数 2 の有限体上で定義された楕円曲線に対しても、上記手順において加算及び 2 倍算の計算に高速な加算及び 2 倍算の計算方法を用いることにより、標数 2 の有限体上で定義された楕円曲線の通常のスカラー倍計算と比べて、高速にスカラー倍計算が実行可能である。

【 0 0 7 9 】

図 2 5 は、図 1 1 の暗号処理システム 1 1 0 1 における秘密情報を用いた暗号処理において、暗号処理経過が漏洩しても秘密情報は漏洩しないスカラー倍計算方法の第 6 実施例を示す図である。図 2 2、図 2 3 及び図 2 4 は、第 6 実施例のスカラー倍計算方法を示すフローチャートである。図 2 2 ～ 図 2 5 を参照して、第 6 実施例を説明する。

【 0 0 8 0 】

スカラー倍計算装置 2 5 0 1 では、点及びスカラー値 2 5 0 7 を入力し、以下の手順でスカラー倍 2 5 0 8 を出力する。ステップ 2 2 0 1 として、繰り返し判定部 2 5 0 6 において繰り返すか否かの判定を行なう為に、初期値として変数 I に 1 を代入する。ステップ 2 2 0 2 として、2 倍算演算部 2 5 0 4 により、点 P の 2 倍点 2 P を計算する。ステップ 2 2 0 3 として、スカラー倍計算装置 2 5 0 1 に入力された点 P とステップ 2 2 0 2 で求めた点 2 P を、点格納部 2 5 0 2 に点の組 (P, 2 P) として格納する。

【 0 0 8 1 】

ステップ 2 2 0 4 として、繰り返し判定部 2 5 0 6 により、変数 I とスカラー値のビット長とが一致するかどうかを判定し、一致すればステップ 2 2 1 3 へ行く。一致しなければステップ 2 2 0 5 へ行く。ステップ 2 2 0 5 として、変数 I を 1 増加させる。ステップ 2 2 0 6 として、ビット値判定部 2 5 0 5 により、スカラー値の I 番目のビットの値が 0 であるか 1 であるかを判定する。そのビットの値が 0 であればステップ 2 4 0 1 へ行く。そのビットの値が 1 であればステップ 2 3 0 1 へ行く。

【0082】

ステップ2301として、演算ランダム化部2509により、加算及び2倍算の計算順序をランダム化する。加算、2倍算の順序で計算を実行する場合はステップ2305へ行く。2倍算、加算の順序で計算を実行する場合はステップ2302へ行く。

【0083】

ステップ2302として、2倍算演算部2504により、点格納部2502に格納されている点の組 $(mP, (m+1)P)$ から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ2303へ行く。ステップ2303として、加算演算部2503により、点格納部2502に格納されている点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ2304へ行く。

【0084】

ステップ2305として、加算演算部2503により、点格納部2502に格納されている点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ2306へ行く。ステップ2306として、2倍算演算部2504により、点格納部2502に格納されている点の組 $(mP, (m+1)P)$ から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ2304へ行く。

【0085】

ステップ2304として、ステップ2303乃至はステップ2305で求めた点 $(2m+1)P$ とステップ2302乃至はステップ2306で求めた点 $(2m+2)P$ を点格納部2502に点の組 $((2m+1)P, (2m+2)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ2204へ戻る。

【0086】

ステップ2401として、演算ランダム化部2509により、加算及び2倍算